The Darknet Index: 2018 Black Hat Edition

NOTABLE DECLINES IN DARKNET EXPOSURE AMONG BLACK HAT EXHIBITORS, BUT DOES A RISKY DARKINT SCORE CORRELATE TO SHARE PRICE PERFORMANCE?

Introduction

DarkOwl uses machine learning to detect and collect data at scale from darknet sites, forums, and channels. In addition to Tor, IRC, I2P, and ZeroNet, DarkOwl collects information from FTP, Amazon S3 Buckets, and transitory paste sites to create its continuously updated database. This DARKINT™ (darknet intelligence) is available via SaaS, API, or data feed to clients wishing to monitor their presence on the darknet.

Using its proprietary database, DarkOwl has developed an algorithm to objectively score how much DARKINT data is publicly available on any particular entity or organization. This DARKINT score is based upon both the quantity and quality of the data we found, as well as its freshness. A higher DARKINT score is worse and implies a higher profile on the darknet, with potential accompanying risk.

DarkOwl has been ranking companies and governments worldwide for almost 2 years now, including companies of the Fortune 500, the German DAX 80, the largest departments and agencies of the US Government, and the largest power utilities. Last year we asked: how does the cybersecurity industry stack up against the commercial enterprises it protects? Accordingly, we ranked the 2017 Black Hat exhibitors by their DARKINT score. The answer to how they ranked turned out to be "better than their customers, with a few notable exceptions". This year, we update our Black Hat scoring for the 2018 attendees. And we also did a small analysis (for the few publicly traded companies at Black Hat) of whether Darknet Index score changes were good proxies to a firm's stock price performance. Even we were surprised at how high the correlation appears.

We examined the 285 Black Hat USA 2018 exhibitors (as compared to the 283 exhibitors in 2017) to see whether they have a markedly different darknet footprints from last year. The improvement, the first we've observed year-over-year for any sample group, was notable with a few exceptions.

TABLE OF CONTENTS

Introduction 1
Methodology 4
The Top 20 6
Conclusions.....8
The Index 9
About Us 20

KEY TAKEAWAYS FROM OUR ANALYSIS

- **The Black Hat exhibitors scored better than expected and actually improved over last year.** The average Darknet Index score of the 2018 Black Hat exhibitor group was 2.1 (vs 2.6 last year), with 30% of Black Hat attendees having no discernible DARKINT score. By comparison, the average Fortune 500 firm scored 8.2 when surveyed eight months ago with 100% of the Fortune 500 firms having a presence on the darknet. Black Hat exhibitors continued to be the best performing industry group we track and the first to register a year-over-year improvement. Even the top 10 exhibitors with the highest scores averaged 9.8 as compared to 12.2 a year ago.

- **AT&T (a new exhibitor) leads the Black Hat DARKINT Index, but Hewlett Packard and Microsoft are not far behind.** With a score of 11.8, AT&T scored highest of all 2018 exhibitors, though this level is far superior to the 15.7 level Microsoft registered as the top scorer a year ago. Microsoft's improvement has been steady, coming in at 12.6 in December and at 10.8 for this survey. We attribute this decrease to the increasingly benign nature of the almost 40,000 darknet mentions of their domain and email domain over the past 90 days on the darknet. HP, which has remained at #2, actually improved more than Microsoft, dropping from 15.4 a year ago and 15.1 in December, to 10.9 this July. IBM at #4 and Booz Allen Hamilton #5 finished out our top 5 scores. Booz Allen Hamilton was our sole "worsening" performer while Amazon's improvement (darknet score dropping from 14.3 to 8.0) was notable.

- **Lower quality of data available on the darknet, not quantity, appears to be driving the scores lower.** The general improvement of Index scores across our survey was not due to less data becoming available on the darknet. In fact, DarkOwl found almost 100,000 mentions of the Black Hat exhibitors in its database over the past 90 days alone, in addition to the 1.2 million older observations. Instead, the generally falling "smoking gun" nature of these most recent results, as determined by our machine learning algorithm, has been driving these lower scores.

- **Vigilance pays off, as shown by the attendee's overall improved standing.** Investing in cybersecurity has tangible index score benefits. While there were exceptions, companies that take information security seriously (like most Black Hat exhibitors), should have less information and less important data on the darknet and, thus, lower Index scores. Our results again confirm this intuition.

"Black Hat exhibitors continue to be the best performing industry group we track."

ABOUT THAT CORRELATION BETWEEN DARKINT SCORES AND SHARE PRICE...

One of the more intriguing new findings is that there may be a correlation between DARKINT score change and stock market performance. Ever since we observed a few companies where such a correllation appeared to exist in our Fortune 500 Darknet Index, we have been intrigued as to whether Darknet Index score trends were systematically correlated to stock price performance. A quick analysis from the very limited number of publicly-traded companies at Black Hat shows that such a correlation may exist. But not in the "if my score is high, that is bad" simple way. Having a high Index score (which implies higher darknet exposure) is certainly not good (think AT&T or Microsoft), but it is also not surprising for large, "attractive" targets. Instead, as the table below shows, having a stagnant but persistently "troubling score" or worse, a steadily increasing score seems to be problematic to public companies. Conversely - a rapidly improving score, even from high levels, is quite good (Amazon is a case in point). Of course this cursory analysis has been performed with too small a data set for statistically significant conclusions. But for those who might otherwise ignore their Darknet Index score thinking, "everyone gets breached" the risks may be larger than expected. The correlation implies that companies which have more information security awareness, processes, and compliance to those policies, will have less data exposed on the darknet and therefore lower DARKINT scores.

TOP PUBLIC EXHIBITORS: DARKINT SCORES VS. SHARE PRICE TRENDS

DARKINT Rank	Name	Stock Price 12/17 to 7/18	Index Score Trend	Index Score Level
1	AT&T Business	-11.75%	flat	high
2	HP Inc.	6.77%	lower	high
3	Microsoft	18.69%	lower	high
7	IBM	-9.63%	flat	moderate
8	Booz Allen Hamilton	15.67%	higher	moderate
9	Raytheon	4.01%	lower	moderate
10	Cisco	13.86%	lower	moderate
11	Symantec	-28.24%	flat	moderate
12	Starbucks	-14.41%	flat	moderate
13	Amazon Web Services	47.44%	much lower	moderate

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, the darknet is purposefully designed to be difficult to trace, and 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.

As a result, the darknet has become a safe harbor for those looking to remain anonymous online, whatever their intentions. A high volume of criminal activity has migrated to the darknet and darknet related sites.

DarkOwl's proprietary platform contains an expansive database of DARKINT content, which can be accessed via a Search platform, API, data feeds. Leveraging this database, we assessed each Black Hat exhibitor, ultimately calculating an overall score for every one with a darknet presence. 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 algorithm yields notable results every time we take a snapshot and perform a static index analysis.

To compile this Index, we ran each Black Hat exhibitor 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 their computed hackishness. We also weighted data based on how recently the data was placed on the darknet; recent results, those found within the last 90 days, were given the most weight, as recent breaches or data leaks containing an organization's proprietary information are often the most prized.

"Using its proprietary database of darknet, deep web, and high-risk surface data, collectively referred to as DARKINT, and its developed algorithms, DarkOwl scored each Black Hat exhibitor based on the quantity and quality of its exposed data, with the higher DARKINT scores signifying a higher exposure profile and greater accompanying risk."

KEY METHODOLOGICAL POINTS

- The Black Hat Darknet Index was constructed with more recent data than our earlier indices, as DarkOwl continues improving its data collection efficiency
- 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 score reflects the value of the target's data less the effectiveness of its protective measures. It is not a "risk of breach" measure. It is more closely aligned to the attractiveness of the target to an attacker while considering the effectiveness of their cybersecurity defenses.
- The size of a single breach is less of a factor than the frequency of breaches over the data collection period.

ALGORITHM

For the purpose of compiling this Index, we used the exact same algorithm as we have for our other indices. Our hackishness algorithm (embedded within our scoring 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 and transitory sites most heavily. All results found in our database were given some weight as per the formula below:

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

DS = DARKINT Score
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

2018 Black Hat Darknet Index: Top 20

The results of our analysis are presented below for the top 20 companies in our 2018 Black Hat Darknet Index. The full ranking of the 285 entrants by their darknet score can be found on page 9. We categorize all companies using the following metrics:

- **DARKINT Rank** - The rank of each company based on their Darknet Index score.
- **Attendee Name** - The entity's name.
- **DARKINT Index Score** - The DARKINT footprint score on which the rankings are based.
- **% New Data**- The percentage of the DARKINT score that was based on data from the last 90 days.

THE 20 BLACK HAT EXHIBITORS WITH THE HIGHEST DARKNET EXPOSURE

DARKINT Rank	Name	DARKINT Score 2018	DARKINT Score 2017	% New Data
1	AT&T Business	20.14	13.24	37.04%
2	HP Inc	18.25	15.09	40.78%
3	Microsoft	16.97	12.62	45.42%
4	University of San Diego	16.68	11.42	27.85%
5	Accenture	16.21	14.32	44.69%
6	Department of Homeland Security	15.46	13.58	25.13%
7	IBM	15.46	9.14	3.96%
8	Booz Allen Hamilton	15.18	4.41	44.74%
9	Raytheon	15.13	10.75	30.99%
10	Cisco	15.12	11.75	12.57%
11	Symantec	15.09	10.32	15.44%
12	Starbucks	15.08	8.95	30.11%
13	Amazon Web Services	15.07	14.27	35.17%
14	Unisys	14.63	N/A	18.13%

THE TOP 20 (CONT.)

DARKINT Rank	Name	DARKINT Score 2018	DARKINT Score 2017	% New Data
15	Sandia National Laboratories	14.62	N/A	11.57%
16	Synopsys	14.59	7.38	3.97%
17	Proviti	14.55	6.88	18.05%
18	VMware	14.44	N/A	36.66%
19	Citrix Systems	14.27	8.05	9.51%
20	McAfee	14.16	7.97	6.50%

KEY OBSERVATIONS ABOUT THE TOP 20

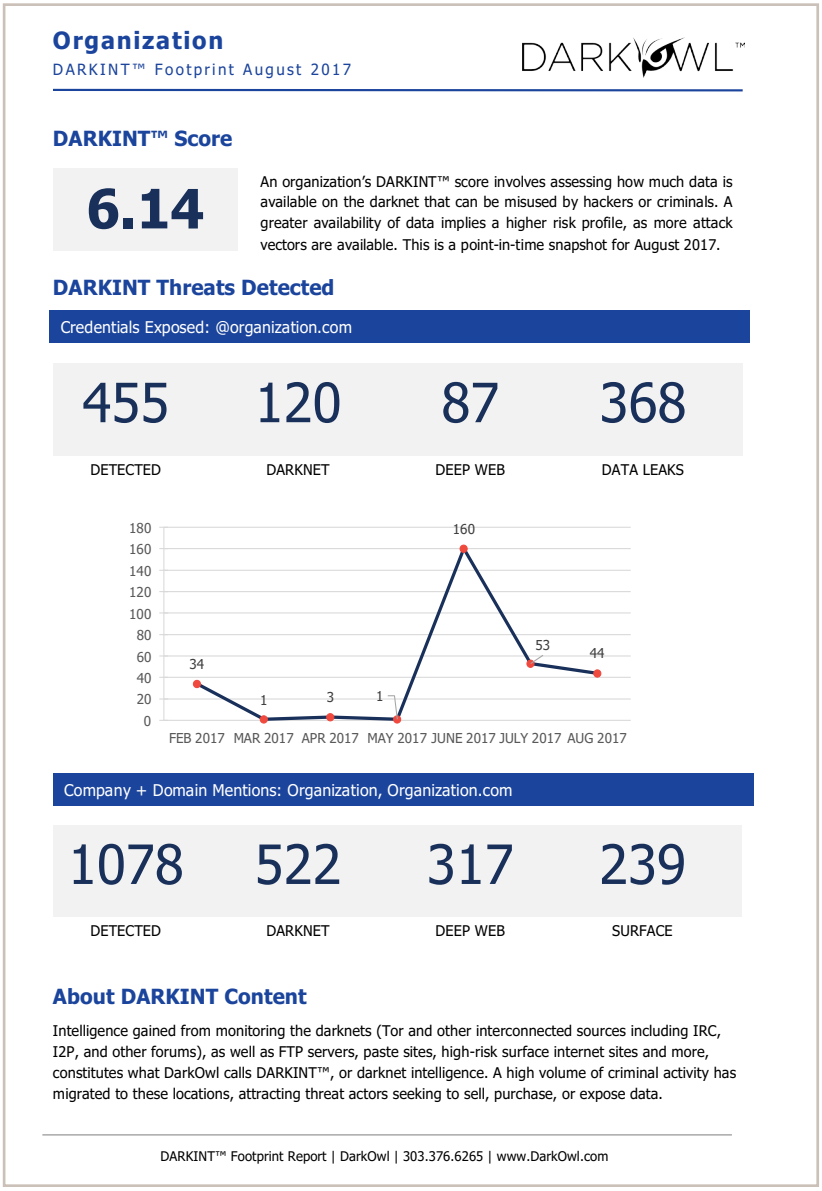
- Unlike the Fortune 500 Darknet Index, whose Top 10 was dominated by Technology companies, the Black Hat Darknet Index Top 20 is populated primarily by technology consultants and larger organizations.
- Average scores of the Black Hat Darknet Index Top 20 (at 8.6) are statistically equivalent to the average score of the entire Fortune 500 from the December 2017 survey (at 8.2).
- Recently posted darknet information drives both overall Index scores and their direction. In general, those with the highest scores and poor Index trends stem from a growing percentage of recent data contributing to their scores.
- Smaller and more recently launched companies may have the media or investment communities' attention, but many have yet to make their debut scoring positively in our index. It would appear that bad actors are more concerned with trading in information from larger entities than conspiring to attack many smaller information security players in the Index.

Conclusions

We live in an era where information breaches often dominate the news. No company or organization is immune from these breaches, and billions of dollars are spent annually in an attempt to protect the valuable data they hold—not even the cybersecurity industry itself. Measuring cybersecurity exposure therefore becomes important for any company seeking to implement a comprehensive cybersecurity strategy and justify a return on their increasing investments. Not surprisingly, the stock market seems to recognize the value of keeping important information off the darknet, though obviously a more comprehensive analysis would be required to determine statistical significance, variance, and causality.

This Black Hat Darknet Index represents a sliver of our DARKINT database which includes information on tens of thousands of additional organizations and individuals. We acknowledge the limitations of any simple scoring analysis, even the one DarkOwl quickly calculates using its Vision platform. A more comprehensive snapshot includes 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 footprint 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. The stock market certainly appears to notice.



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 2018 Black Hat Exhibitors

DARKINT Rank	Name	DARKINT Score
1	AT&T Business	11.78
2	HP Inc.	10.90
3	Microsoft Corporation	10.84
4	University of San Diego	9.99
5	Accenture	9.98
6	Department of Homeland Security	9.29
7	IBM	9.12
8	Booz Allen Hamilton	8.91
9	Raytheon	8.73
10	Cisco	8.62
11	Symantec	8.57
12	Starbucks	8.19
13	Amazon Web Services	7.97
14	Unisys	7.71
15	Sandia National Laboratories	7.50
16	Synopsys	7.16
17	Protiviti	7.08
18	VMware	6.82
19	Citrix Systems	6.81
20	McAfee	6.66
21	Neustar	6.34
22	Gemalto	6.30
23	Informatica	6.23
24	NVIDIA	6.11
25	UMUC	5.81

DARKINT Rank	Name	DARKINT Score
26	F5 Networks	5.74
27	RSA	5.74
28	Fortinet	5.70
29	Check Point Software	5.54
30	NETSCOUT | Arbor	5.50
31	Aruba: a Hewlett Packard Enterprise company	5.34
32	Spirent Communications	5.29
33	Trend Micro	5.28
34	Sirius Security	5.23
35	Federal Bureau of Investigation	5.17
36	Sophos Inc	5.03
37	Watchguard Technologies	5.01
38	Cloakware by Irdeto	4.98
39	Radware	4.94
40	SonicWall	4.93
41	Flexera	4.83
42	O'Reilly Media: Inc.	4.74
43	Infoblox	4.66
44	Splunk	4.64
45	Webroot	4.62
46	LGS Innovations	4.59
47	Barracuda Networks: Inc.	4.59
48	Trustwave	4.57
49	Palo Alto Networks	4.50
50	ServiceNow	4.50
51	Tripwire	4.39

DARKINT Rank	Name	DARKINT Score
52	Cloudera	4.38
53	Endace	4.33
54	Bitdefender	4.26
55	Rapid7	4.26
56	Comodo Cybersecurity Solutions	4.21
57	Qualys	4.03
58	ESET	3.99
59	Bomgar	3.93
60	Mimecast	3.89
61	Afilias plc	3.79
62	FireEye	3.78
63	Proofpoint: Inc.	3.75
64	(ISC)¬≤	3.74
65	Varonis	3.71
66	Pluralsight LLC	3.66
67	A10 Networks	3.64
68	ISACA	3.61
69	Gigamon	3.58
70	Devo	3.54
71	SageNet	3.48
72	Corvil	3.47
73	Intertrust	3.45
74	AlienVault	3.44
75	SecureAuth + Core Security	3.43
76	ForeScout Technologies	3.43
77	Stroz Friedberg	3.39

DARKINT Rank	Name	DARKINT Score
78	LogRhythm	3.36
79	Veracode	3.32
80	OWASP	3.31
81	Skybox Security	3.29
82	Cloudflare	3.27
83	Duo Security	3.24
84	Centrify	3.23
85	BeyondTrust	3.20
86	Fidelis Cybersecurity	3.20
87	Electronic Frontier Foundation (EFF)	3.18
88	Fasoo	3.16
89	Netwrix	3.14
90	Code42 Software	3.08
91	Solarflare Communications	3.07
92	Radiant Logic	3.06
93	Thycotic	3.03
94	WhiteHat Security	3.02
95	Venafi	3.01
96	MediaPro	2.94
97	DigiCert	2.89
98	Garrison Inc.	2.89
99	OPSWAT	2.87
100	Ziften	2.79
101	Continuum Managed Services	2.77
102	Okta	2.75
103	Recorded Future	2.71

DARKINT Rank	Name	DARKINT Score
104	netSPI	2.71
105	ReliaQuest	2.69
106	Guavus	2.60
107	Belarc	2.58
108	DomainTools	2.51
109	InfoArmor	2.47
110	Tenable	2.45
111	eSentire	2.38
112	Bromium	2.32
113	ISSA International	2.25
114	Cloud Security Alliance (CSA)	2.25
115	3Pillar Global	2.21
116	Faraday	2.21
117	Checkmarx	2.17
118	DFLabs	2.17
119	Deep Secure	2.12
120	Sumo Logic	2.11
121	JASK	2.08
122	ExtraHop Networks	2.03
123	Coalfire	1.98
124	Securonix	1.98
125	Semmle	1.92
126	KnowBe4	1.92
127	NSS Labs	1.92
128	Yubico	1.80
129	Adaptiva	1.80

DARKINT Rank	Name	DARKINT Score
130	Brinqa	1.73
131	Forcepoint	1.65
132	Onapsis	1.65
133	CrowdStrike	1.57
134	Wombat Security: a division of Proofpoint	1.56
135	Lastline	1.46
136	Endgame	1.46
137	WhiteSource	1.46
138	ObserveIT	1.46
139	Authentic8	1.46
140	CounterTack	1.46
141	PhishLabs	1.35
142	Spirion	1.34
143	Malwarebytes	1.22
144	eLearnSecurity	1.21
145	Fastly: Inc.	1.21
146	Optiv Security	1.21
147	Thales eSecurity	1.21
148	iboss	1.20
149	CyberArk Software	1.04
150	Digital Shadows	1.04
151	Cybereason	1.04
152	Detectify	1.04
153	HackerOne	0.83
154	Interset	0.82
155	NRI SecureTechnologies	0.82

DARKINT Rank	Name	DARKINT Score
156	ReversingLabs	0.82
157	Signal Sciences	0.82
158	Elastic	0.54
159	Kudelski Security	0.52
160	Cavirin	0.52
161	Synack	0.52
162	Attivo Networks	0.52
163	BigID	0.52
164	Flashpoint	0.52
165	Joe Security LLC	0.52
166	Netskope	0.52
167	SAASPASS	0.01
168	Menlo Security	0.01
169	Barkly	0.01
170	Netsparker	0.01
171	Nominet	0.01
172	PolySwarm	0.01
173	LookingGlass	0.01
174	Siemplify	0.01
175	Digital Guardian	0.01
176	PerimeterX	0.01
177	Sysdig	0.01
178	Valimail	0.01
179	Carbon Black	0.01
180	Cylance	0.01
181	Jscrambler	0.01

DARKINT Rank	Name	DARKINT Score
182	NowSecure	0.01
183	Darktrace	0.01
184	Twistlock	0.01
185	Armis Inc	0.01
186	Ataata	0.01
187	Bishop Fox	0.01
188	Bracket Computing	0.01
189	DarkMatter	0.01
190	One Identity	0.01
191	Verodin	0.01
192	77 Element	0.00
193	Acalvio Technologies	0.00
194	Allure Security	0.00
195	Anomali	0.00
196	Area 1 Security	0.00
197	AttackIQ	0.00
198	Awake Security	0.00
199	Binary Defense	0.00
200	Bitglass	0.00
201	BluVector	0.00
202	BTB Security	0.00
203	CBI	0.00
204	CIAS: UTSA	0.00
205	Cofense	0.00
206	Cognigo	0.00
207	Contrast Security	0.00

DARKINT Rank	Name	DARKINT Score
208	Cord3 Innovation	0.00
209	Corelight	0.00
210	Cyber Intelligence House	0.00
211	CyberGRX	0.00
212	Cyberinc	0.00
213	CyberVista	0.00
214	Cymmetria	0.00
215	Cyxtera Technologies	0.00
216	DarkOwl	0.00
217	Deep Instinct	0.00
218	Demisto	0.00
219	Digital Defense: Inc.	0.00
220	Distil Networks	0.00
221	DriveLock	0.00
222	Edgewise Networks	0.00
223	enSilo	0.00
224	Executive Women's Forum	0.00
225	Farsight Security	0.00
226	FFRI North America: Inc.	0.00
227	Fractal Industries	0.00
228	FunCaptcha	0.00
229	GuardSquare	0.00
230	Gurucul	0.00
231	Illumio	0.00
232	Infocyte	0.00
233	Intezer	0.00

DARKINT Rank	Name	DARKINT Score
234	IntSights	0.00
235	IRONSCALES	0.00
236	Javelin Networks	0.00
237	Kenna Security	0.00
238	LogicHub	0.00
239	NanoVMs	0.00
240	Nehemiah Security	0.00
241	Netsurion	0.00
242	NeuVector Container Security	0.00
243	Nyotron Security	0.00
244	Obsidian Security	0.00
245	Passus & Smartvide	0.00
246	PFP Cybersecurity	0.00
247	Phantom	0.00
248	Polarity	0.00
249	PreVeil	0.00
250	Privoro	0.00
251	ProtectWise	0.00
252	Qadium	0.00
253	Remediant	0.00
254	Resolve Systems	0.00
255	Ribbon Communications	0.00
256	RiskIQ	0.00
257	RiskSense	0.00
258	RiskVision	0.00
259	SafeBreach	0.00

DARKINT Rank	Name	DARKINT Score
260	ScaleFT	0.00
261	Secure Channels Inc.	0.00
262	SecurityGate	0.00
263	SecurityScorecard	0.00
264	SentinelOne	0.00
265	ShieldX Networks	0.00
266	Soliton Cyber and Analytics: Inc.	0.00
267	SpecterOps	0.00
268	Swimlane	0.00
269	tCell.io	0.00
270	Terbium Labs	0.00
271	Threat Intelligence - Evolve Security Automation	0.00
272	Threat Stack	0.00
273	Threat X	0.00
274	ThreatConnect	0.00
275	Tigera	0.00
276	Trustlook	0.00
277	Uplevel Security	0.00
278	Vectra	0.00
279	VMRay	0.00
280	wolfSSL	0.00
281	Women in Security and Privacy	0.00
282	Women‚Äôs Society of Cyberjutsu	0.00
283	XM Cyber	0.00
284	ZeroFOX	0.00
285	Zingbox	0.00

About DarkOwl

DarkOwl is based in Denver, Colorado providing DARKINT threat intelligence data 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 DARKINT content available to commercial users.