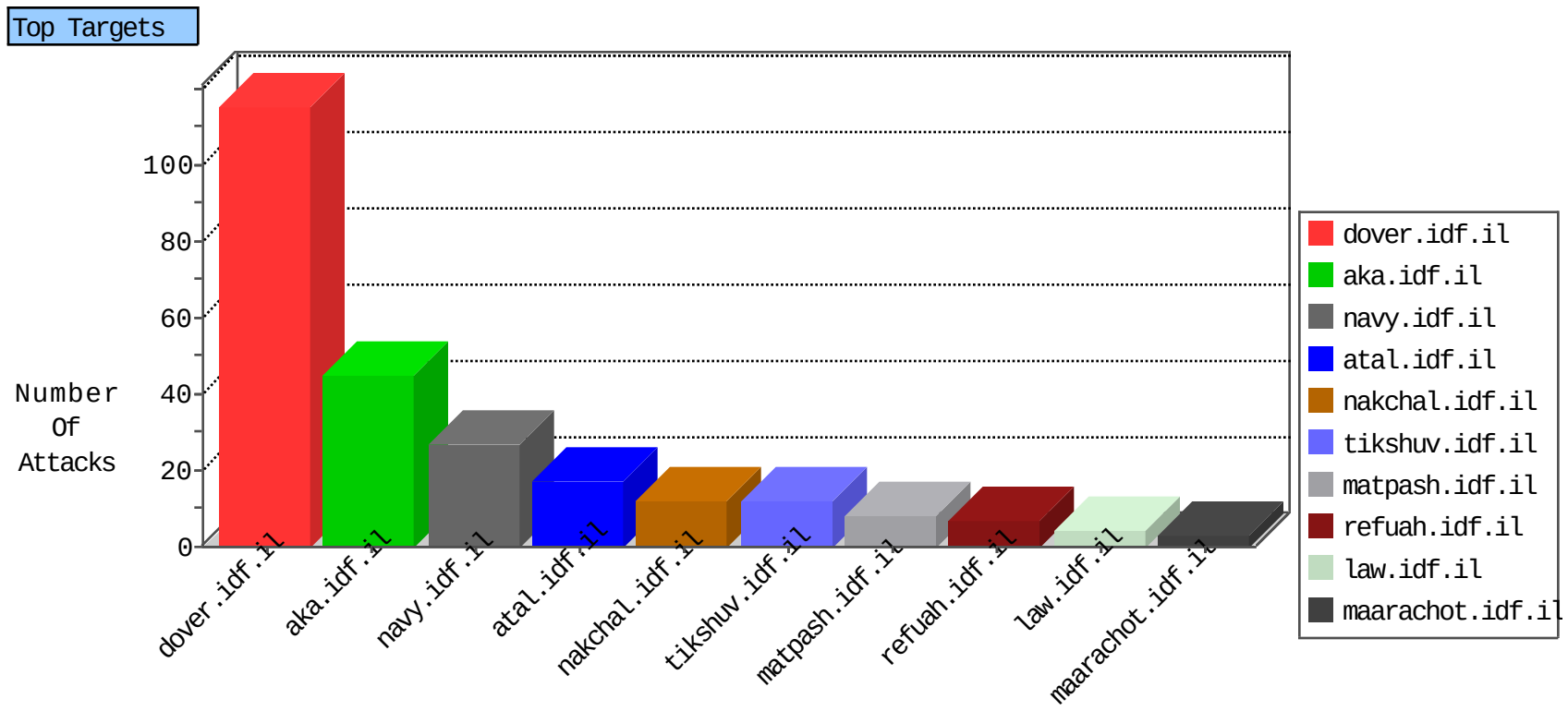
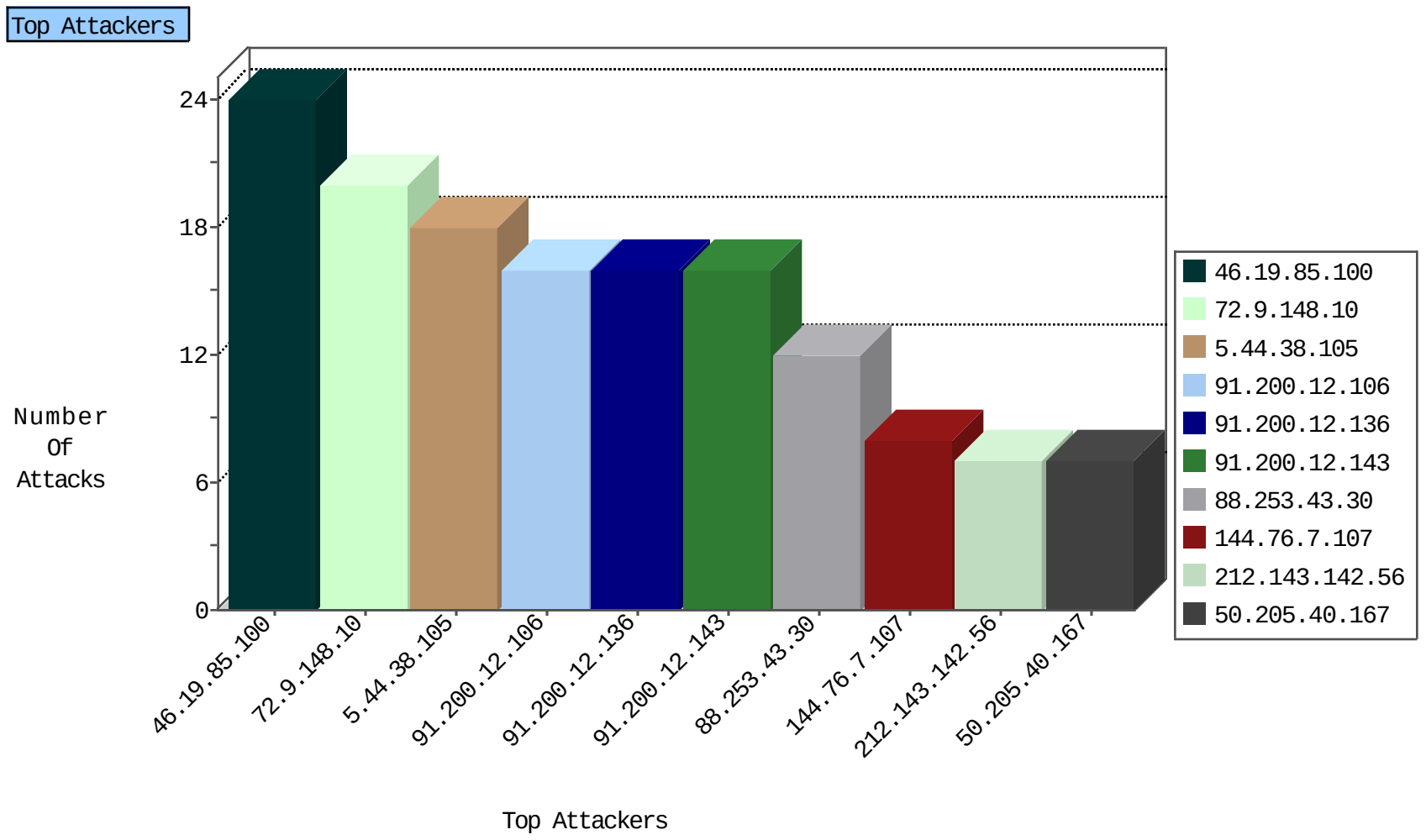
03-08-2016-01:12:56 to 03-08-2016-02:12:56

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-08-2016-01:12:56 to 03-08-2016-02:12:56

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.223.77	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
79.176.197.214	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.97.254.50		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
222.186.21.112	China	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-08-2016-01:12:56 to 03-08-2016-02:12:56

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.205.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
144.76.7.107	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.69.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.7.107	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.7.107	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.7.107	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
185.3.147.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
88.253.43.30	Turkey	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Block	1
188.165.15.66	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
42.101.152.49	China	147.237.77.176	matpash.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-01:12:56 to 03-08-2016-02:12:56

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.59.252.185	147.237.77.216	Germany	dover.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.114	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN Potential SSH Scan	1
188.136.144.104	147.237.0.15	Iran, Islamic Republic of	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
187.245.56.142	147.237.77.227	Mexico	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
219.92.36.38	147.237.77.61	Malaysia	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
188.136.144.104	147.237.0.15	Iran, Islamic Republic of	kosher-kravi.idf.i	ET SCAN NMAP -sS window 4096	1
188.136.144.104	147.237.0.15	Iran, Islamic Republic of	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1

03-08-2016-01:12:56 to 03-08-2016-02:12:56

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.44.38.105	Azerbaijan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
50.205.40.167	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.188.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
91.200.12.136	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
91.200.12.106	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
91.200.12.106	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
89.145.95.42	United Kingdom	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.185.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.3.147.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.154.170.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.176.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.173.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.147.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.25.83.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
212.25.83.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
80.246.136.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.73	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.57.9.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.16.11.27	Germany	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.230	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.145	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.147.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.146	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.138.1.218	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.67.152.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
51.254.44.137	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.158	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.138.179.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
190.191.248.75	Argentina	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
51.254.44.137	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.159	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-08-2016-01:12:56 to 03-08-2016-02:12:56

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.253.43.30	Turkey	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 88.253.43.30	Block	4
88.253.43.30	Turkey	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
88.253.43.30	Turkey	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 88.253.43.30	Block	2
2.52.30.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
207.46.13.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
184.154.48.210	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 184.154.48.210	Block	1
78.12.192.93	Italy	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.48	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/105595.pdf	Block	1
197.48.72.82	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
5.62.199.4	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13467-en/dover.aspx'	Block	1
184.154.48.210	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
78.12.192.93	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.53	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/112296.pdf	Block	1
197.48.72.82	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
88.253.43.30	Turkey	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
66.249.66.29	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.142.204.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.82.200.91		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
88.253.43.30	Turkey	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
66.249.64.235	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
197.48.72.82	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.48.72.82	Block	1
109.186.172.166	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
66.249.73.190	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.73.190	Block	1
41.34.251.100	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.138.1.218	Germany	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/robots.txt	Block	1
66.249.64.253	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 66.249.64.253 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
202.46.58.164	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9366-he/refuah.aspx	Block	1
180.76.15.24	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9238-he/refuah.aspx	Block	1
73.143.247.211	United States	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
41.34.251.100	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
197.48.72.82	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.64.253	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.62.199.4	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1

03-08-2016-01:12:56 to 03-08-2016-02:12:56