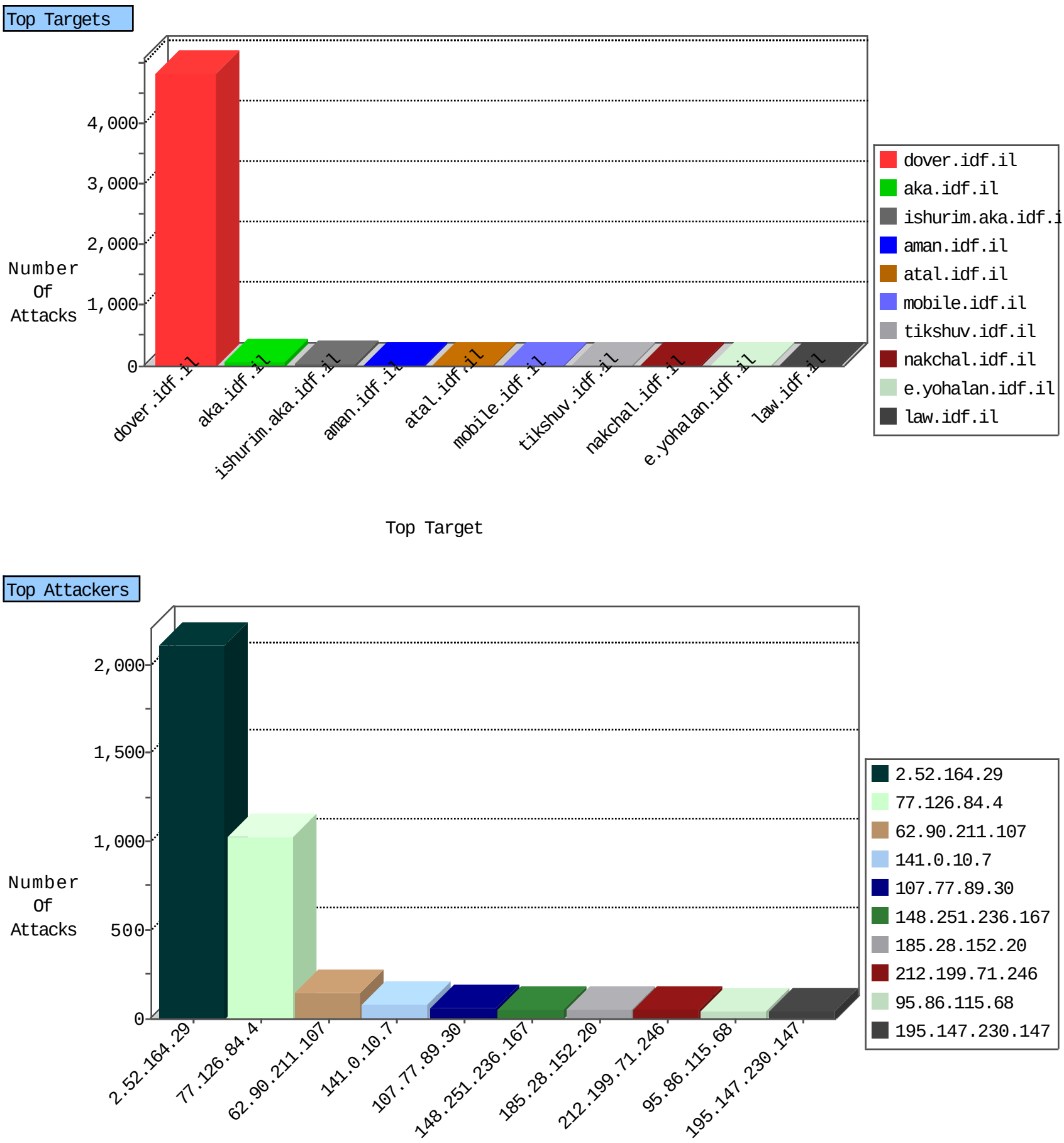
05-07-2015-18:03:08 to 05-07-2015-19:03:08

IDF Under Attack
05-07-2015-18:03:08



05-07-2015-18:03:08 to 05-07-2015-19:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
109.65.142.4	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	247
46.120.73.155	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
84.94.96.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
85.65.122.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
5.28.182.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.179.159.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
46.19.85.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

05-07-2015-18:03:08 to 05-07-2015-19:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	30
37.130.227.133	United Kingdom	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	10
197.37.115.59	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
176.58.100.98	United Kingdom	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.63	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.163.235.228	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
118.137.161.7	Indonesia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.241.160.132	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.i	DVRep_B-N_60_100	Block	1
82.213.57.145	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
5.135.85.23	France	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
101.251.236.91	China	147.237.77.234	halag.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
211.20.239.55	Taiwan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1

05-07-2015-18:03:08 to 05-07-2015-19:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.79	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
79.182.203.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.52.164.29	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
67.159.16.2	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
58.97.2.66	Thailand	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
183.136.216.3	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.3	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
92.53.45.135	Macedonia, the Former Yugoslav Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.171.167	Netherlands	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
67.159.16.2	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
58.97.2.66	Thailand	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.189.245	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.65.112.209	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
92.53.45.135	Macedonia, the Former Yugoslav Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.171.167	Netherlands	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

05-07-2015-18:03:08 to 05-07-2015-19:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.164.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2111
77.126.84.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1030
62.90.211.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	144
141.0.10.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
107.77.89.30	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
185.28.152.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
212.199.71.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
148.251.236.167	Germany	147.237.77.216	dover.idf.il	SAM rule	drop	drop	47
95.86.115.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
195.147.230.147	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
46.116.74.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
46.19.85.137	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
99.238.32.134	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
31.186.228.68	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.91	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
193.43.246.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
209.2.26.207	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
31.186.228.65	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.19.85.234	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
85.130.193.195	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	11
79.182.189.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.142.73.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
82.80.17.163	Israel	147.237.72.156	aman.idf.il	SAM rule	drop	drop	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
113.92.114.232	China	147.237.77.216	dover.idf.il		drop	drop	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
74.6.254.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
31.186.228.170	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.64.253	United States	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.177.166.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.92	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.87	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
193.43.245.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
85.64.148.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.90	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
181.214.50.44		147.237.72.166	aka.idf.il	PHP Attempt	Block	5
37.26.147.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	4
84.228.221.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	3
212.143.169.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	3
213.57.169.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
173.206.77.224	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
148.251.236.167	Germany	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 148.251.236.167	Block	2
95.86.78.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
148.251.236.167	Germany	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 148.251.236.167	Block	2
66.249.93.204	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to himush.atal.idf.il/webresource.axd	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10641-he/dover.aspx	Block	1
104.131.209.252		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unknown Parameter 1ff7b328 in aka.idf.il/iturim/asp/results.asp	None	1
79.176.36.154	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
113.92.114.232	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
46.120.220.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter mouduleToGoTo in www.aka.idf.il/main/giyus/login.aspx	None	1
85.250.12.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
180.76.4.40	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.93.212	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to himush.atal.idf.il/scriptresource.axd	Block	1
148.251.236.167	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.67.78	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
104.131.234.204		147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
79.180.147.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-index08.stm	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
148.251.236.167	Germany	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
50.144.1.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
87.69.233.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
149.78.138.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.174.169	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.180.179.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/yoman/	Block	1
148.251.236.167	Germany	147.237.77.216	dover.idf.il	Illegal HTTP Version Ã–Â”Ã–Â–Ã–Â™Ã–Â›Ã–Â¨Ã–Â•Ã–ÂŸ Ã–Âœ Ã–Â–Ã–Â–Ã–ÂœÃ–ÂœÃ–Â™ Ã–ÂžÃ– HTTP/1.1	Block	1
61.135.190.68	China	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17//	Block	1
188.138.17.205	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/wante.stm	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-16897-en/dover.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	1
2.54.178.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.201.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
80.246.130.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.90.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1

05-07-2015-18:03:08 to 05-07-2015-19:03:08