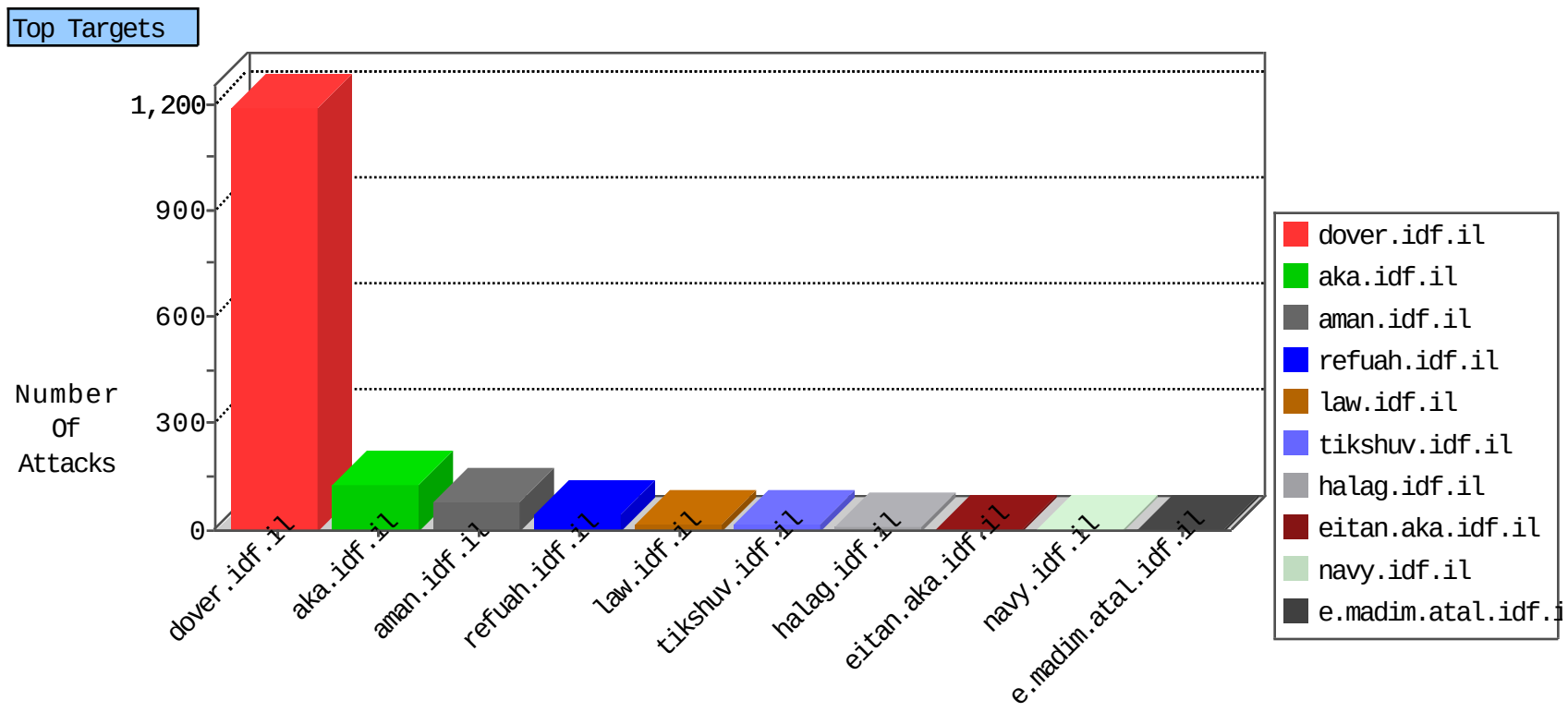
05-02-2015-13:03:06 to 05-02-2015-14:03:06

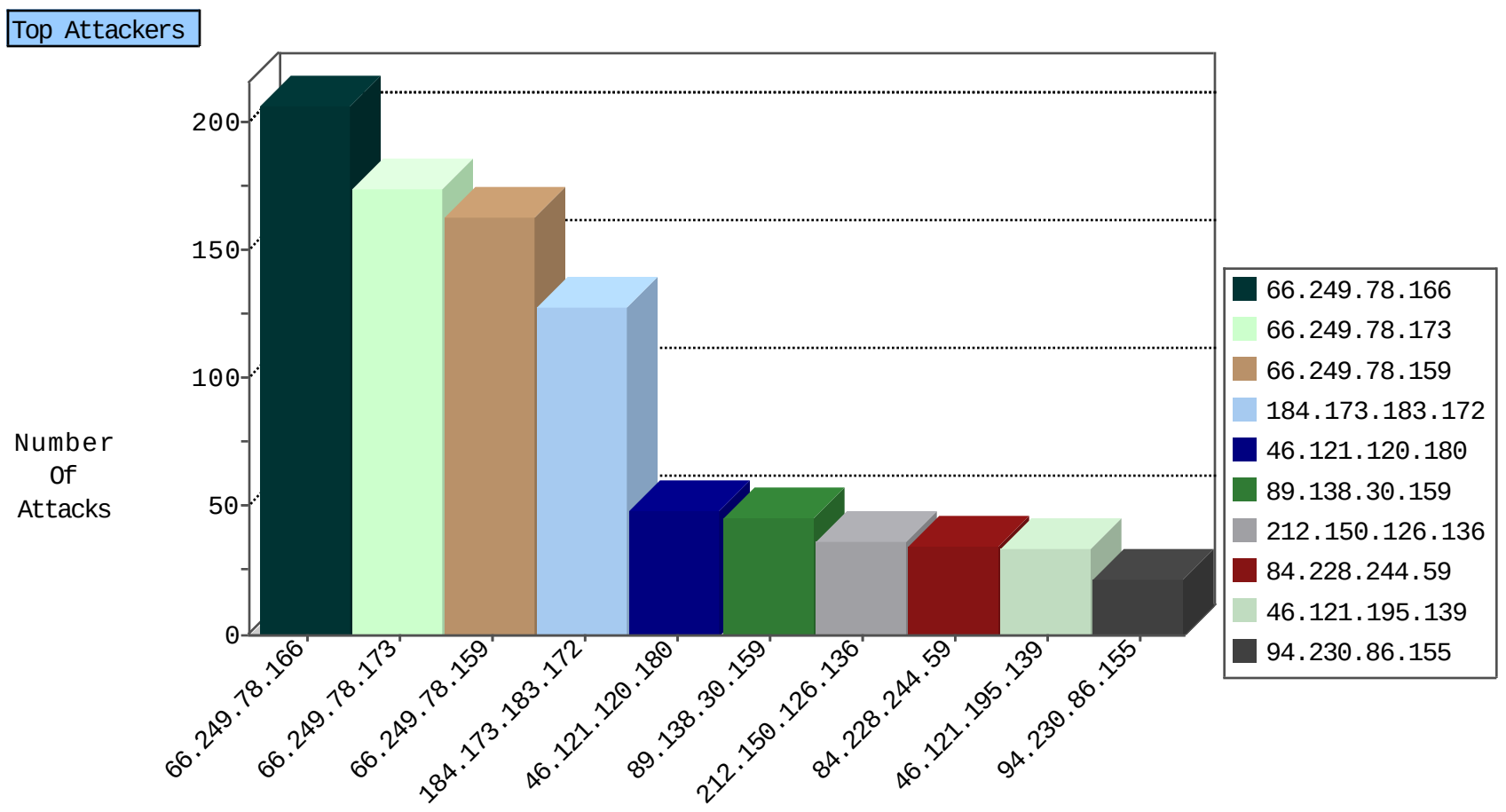
IDF Under Attack
05-02-2015-13:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

05-02-2015-13:03:06 to 05-02-2015-14:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	760
46.121.120.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	409
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	115
89.138.242.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
10.0.0.6		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
146.185.239.100	Russian Federation	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
192.3.206.130	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
46.19.85.75	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
124.232.142.220	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

05-02-2015-13:03:06 to 05-02-2015-14:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	128
89.138.30.159	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.22.130.185	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.115.82.54	Anonymous Proxy	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
212.235.68.141	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
72.91.210.24	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
94.230.86.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.136.227.24	Germany	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-13:03:06 to 05-02-2015-14:03:06

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	5
37.142.98.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.178.9.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
77.125.166.70	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
118.144.129.11	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
118.144.129.11	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
178.32.251.100	France	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
118.144.129.11	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
118.144.129.11	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	Kazakstan	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
183.232.128.156	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
118.144.129.11	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1

05-02-2015-13:03:06 to 05-02-2015-14:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	158
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	141
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	130
212.150.126.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
89.138.30.159	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	36
84.228.244.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
46.121.195.139	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	34
5.156.8.240	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
149.78.72.59	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.93.216	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
109.64.52.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
87.69.20.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.181.36.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
94.230.86.155	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
46.19.85.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
149.78.72.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
220.227.112.205	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
94.230.86.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
94.159.212.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.117	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.117	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.65.142.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
76.173.28.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
188.161.114.3	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
87.69.81.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.52.1.140	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.228.246.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
213.55.115.112	Ethiopia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
89.138.30.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.178.162.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.250.101.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
94.230.86.155	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
213.57.41.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	22
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	21
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	16
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
87.69.162.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.162.9	Block	5
87.68.41.135	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 87.68.41.135	Block	4
46.120.212.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
82.166.100.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
94.230.86.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
213.55.115.112	Ethiopia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	2
78.46.203.72	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.181.120.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unknown Parameter 9ff3fe30 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.195.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.229.164.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
66.249.81.227	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
176.12.150.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-18261-en/dover.aspx	Block	1
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: catid%5Cu003d59336 in www.aka.idf.il/main/giyus/general.aspx	Block	1
37.26.147.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
82.166.235.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7783-he/nakhal.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21498-h	Block	1
68.180.228.251	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19936-ar/kkkkkkk=a8c2649bkkkkkkk_a8c2649b	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/870-2339-he/patzar.aspx	Block	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
84.108.65.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;sOrderBy in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1381-17403-he/dover.aspx	Block	1
188.138.17.205	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/164-4312-he/patzar.aspx	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
149.78.125.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
84.108.153.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1