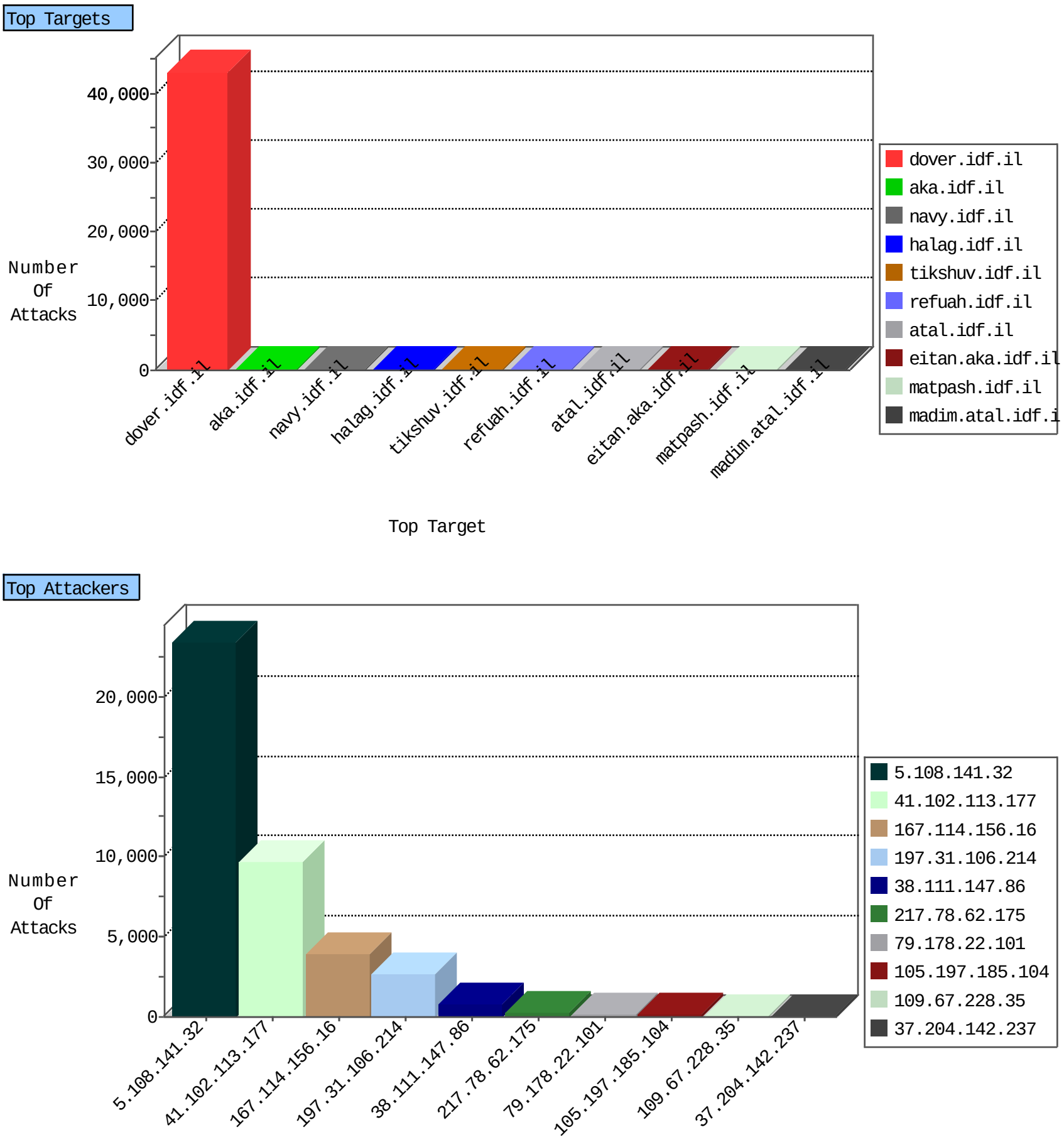
04-10-2016-01:05:03 to 04-10-2016-02:05:03

IDF Under Attack Daily Report



04-10-2016-01:05:03 to 04-10-2016-02:05:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3889
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1538
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	414
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	76
105.154.161.197	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	25
41.141.167.94	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	17
41.141.81.207	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	5
41.249.62.47	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
173.208.197.252	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
74.91.18.46	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
41.251.172.209	Morocco	147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	2
173.208.197.254	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
74.91.23.110	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
107.150.32.58	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
74.91.17.180	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
41.141.163.82	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
82.145.208.69	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
41.251.149.86	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
41.224.66.164	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
41.141.161.39	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1

04-10-2016-01:05:03 to 04-10-2016-02:05:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.249.62.47	Morocco	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	2
199.30.24.182	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.91.170.122	Saudi Arabia	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
185.106.92.47	Russian Federation	147.237.77.235	sviva.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
41.249.62.47	Morocco	147.237.77.216	dover.idf.il	3999: HTTP: Cross Site Scripting Attack in HTTP Header	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-01:05:03 to 04-10-2016-02:05:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
62.47.237.29	147.237.8.27	Austria	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
185.106.92.47	147.237.77.235	Russian Federation	sviva.idf.il	ET WEB_SERVER Muieblackcat scanner	1
66.240.213.93	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
62.47.237.29	147.237.8.14	Austria	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.47.237.29	147.237.0.16	Austria	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.47.237.29	147.237.77.233	Austria	atal.idf.il	ET SCAN Potential SSH Scan	1
41.249.62.47	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP server-info access	1
62.47.237.29	147.237.77.226	Austria	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
13.92.187.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
62.47.237.29	147.237.77.212	Austria	e.dover.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
62.47.237.29	147.237.77.170	Austria	maarachot.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
62.47.237.29	147.237.76.176	Austria	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
186.124.175.187	147.237.0.33	Argentina	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.47.237.29	147.237.76.31	Austria	nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.210.24.10	147.237.0.34	Malaysia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.47.237.29	147.237.8.24	Austria	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.47.237.29	147.237.0.19	Austria	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
62.47.237.29	147.237.77.243	Austria	mobile.idf.il	ET SCAN Potential SSH Scan	1
62.47.237.29	147.237.0.15	Austria	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.47.237.29	147.237.77.227	Austria	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
62.47.237.29	147.237.77.216	Austria	dover.idf.il	ET SCAN Potential SSH Scan	1
13.92.187.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
62.47.237.29	147.237.77.179	Austria	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
62.47.237.29	147.237.77.121	Austria	e.navy.idf.il	ET SCAN Potential SSH Scan	1
62.47.237.29	147.237.76.42	Austria	refuah.idf.il	ET SCAN Potential SSH Scan	1

04-10-2016-01:05:03 to 04-10-2016-02:05:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21874
41.102.113.177	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9687
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1114
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		reject	954
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	836
217.78.62.175	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	232
79.178.22.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	151
105.197.185.104	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
109.67.228.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
37.204.142.237	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	48
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
157.55.39.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.213.78.152	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
5.102.242.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
162.157.233.101	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
105.107.248.108	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.141.167.94	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
41.141.167.94	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
41.141.161.39	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
141.0.15.207	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
79.177.241.124	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
185.27.105.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
146.185.56.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
194.187.168.193	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
108.41.16.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
69.125.172.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.53.21.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
5.102.236.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.64.233.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.26.146.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
207.46.13.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.65.55.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
165.124.144.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
105.110.53.155	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
89.138.195.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.249.62.47	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.249.62.47	Block	6
219.155.147.158	China	147.237.76.86	navy.idf.il	PHP Attempt	Block	5
219.155.147.158	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	4
219.155.147.158	China	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 219.155.147.158	Block	4
46.19.85.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
219.155.147.158	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 219.155.147.158	Block	3
219.155.147.158	China	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 219.155.147.158	Block	3
219.155.147.158	China	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	3
109.253.206.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
8.37.71.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/&gws_rd=cr&ei=v3ujv5k5d4jeavqbjaac	Block	1
219.155.147.158	China	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 219.155.147.158	Block	1
109.64.106.34	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.91.18.46	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.tt782.com/	Block	1
219.155.147.158	China	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
219.155.147.158	China	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
41.141.167.94	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7	Block	1
2.91.170.122	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-ar/dover.aspx	Block	1
89.138.195.243	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
219.155.147.158	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/plus/mytag_js.php	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/62933.pdf	Block	1
31.178.144.59	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
219.155.147.158	China	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
74.91.23.110	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
219.155.147.158	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/bbs/utility/convert/index.php	Block	1
219.155.147.158	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
41.249.62.47	Morocco	147.237.77.216	dover.idf.il	Malformed URL www.acunetix.wvs:443	Block	1
169.229.3.90	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/rec.dat	Block	1
2.91.170.122	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation Language in www.idf.il/shared/ajax/getemergencybanner.aspx	Block	1
89.139.175.163	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
31.178.144.59	Poland	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
110.86.186.223	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
79.177.241.124	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
219.155.147.158	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/plus/mytag_js.php	Block	1
173.208.197.254	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
2.91.170.122	Saudi Arabia	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
105.154.161.197	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
41.141.161.39	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
156.203.28.46	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
45.33.133.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
2.91.170.122	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin	Block	1
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
107.150.32.58	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on www.tt782.com/	Block	1
74.91.17.180	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.tt985.com/	Block	1
219.155.147.158	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/plus/mytag_js.php	Block	1
41.141.163.82	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
219.155.147.158	China	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 219.155.147.158	Block	1