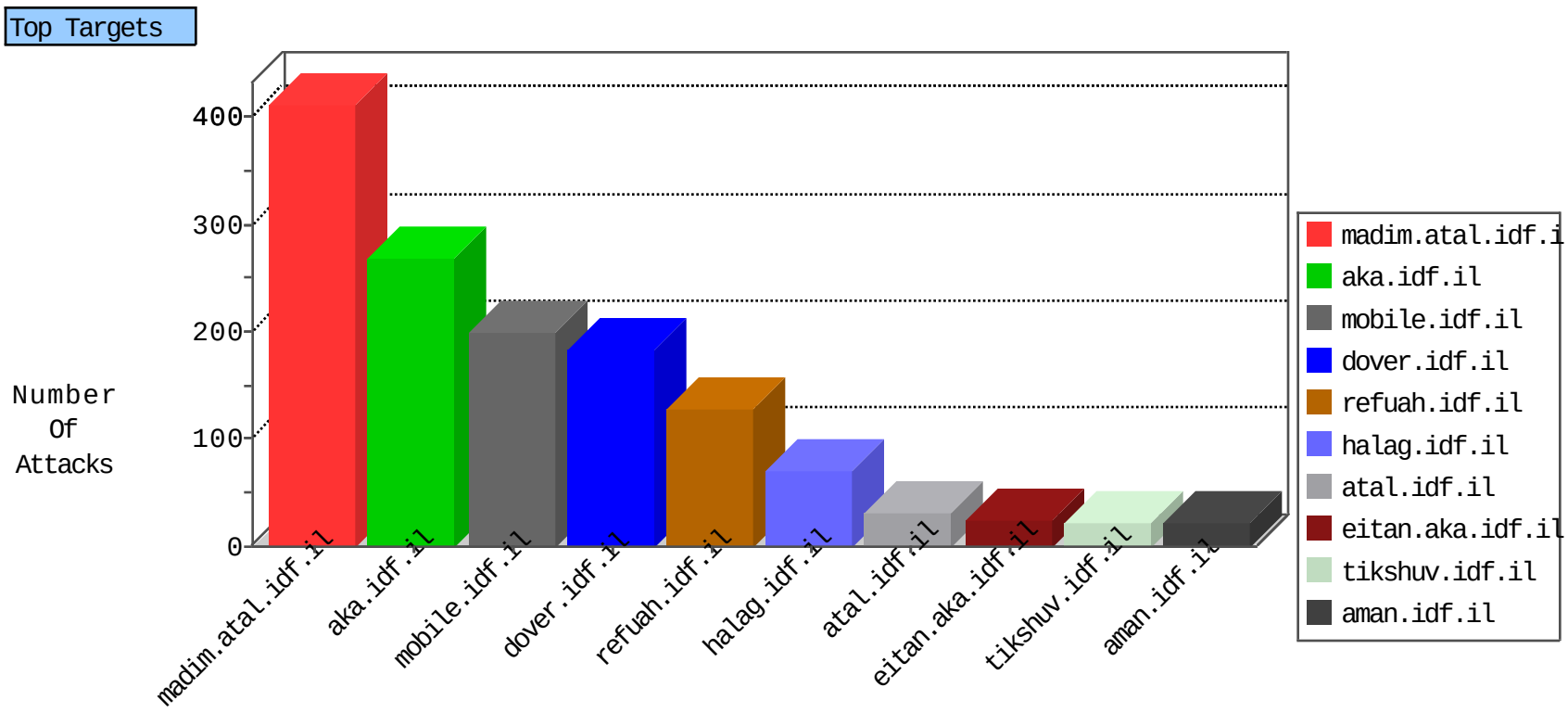
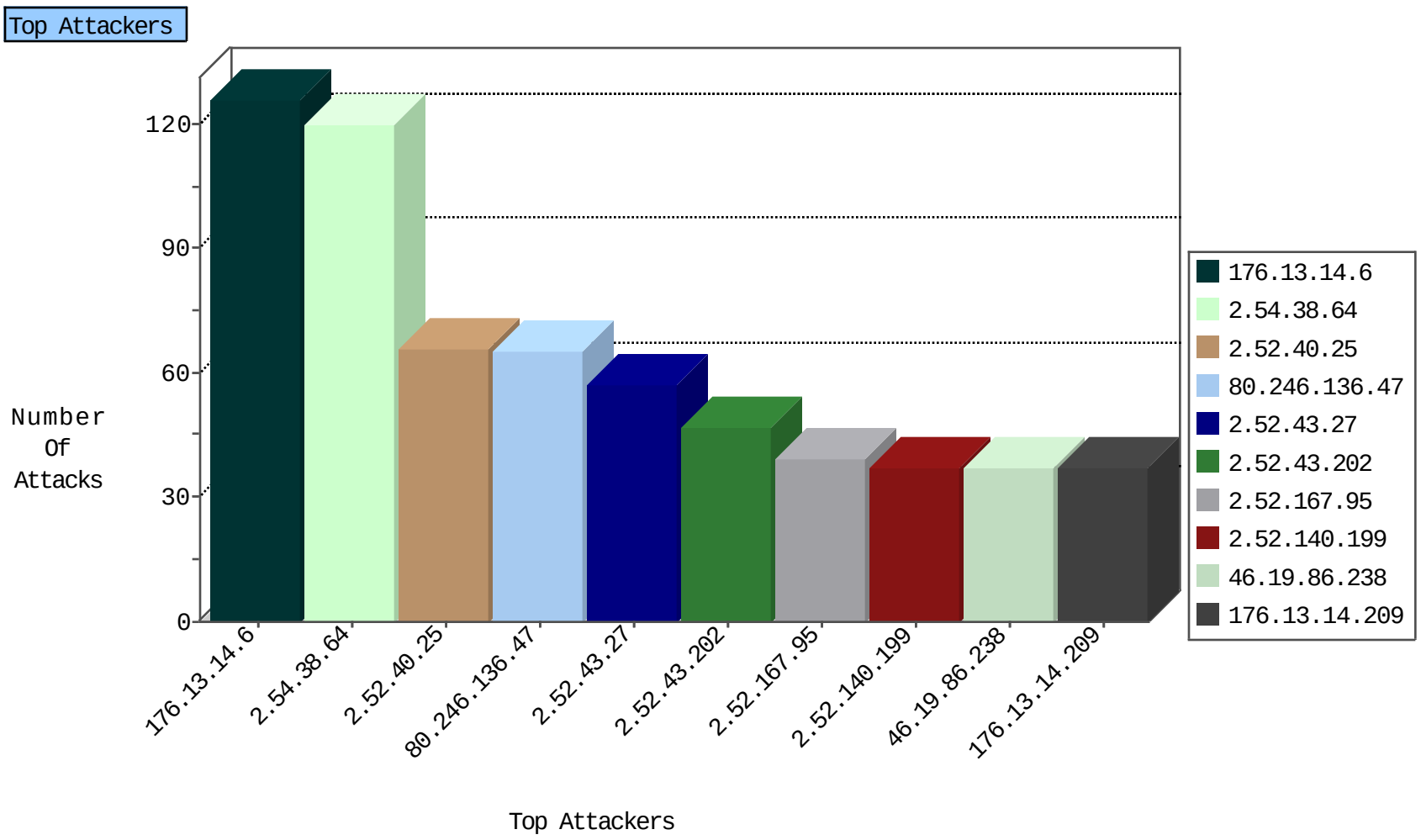
03-06-2016-12:04:02 to 03-06-2016-13:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2016-12:04:02 to 03-06-2016-13:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.40.4.45		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
23.94.69.234	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
185.40.4.45		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
23.94.69.234	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
212.71.235.23	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.132	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
108.186.168.25	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1

03-06-2016-12:04:02 to 03-06-2016-13:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.133.83	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
2.54.131.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
109.67.143.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
103.40.163.112		147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-06-2016-12:04:02 to 03-06-2016-13:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.120.126.111	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.16.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.106.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.184.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.50.141.152	147.237.0.16	United Arab Emirates	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
198.180.198.185	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
198.180.198.185	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
178.42.1.107	147.237.76.31	Poland	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.218.241.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.126.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.87.243.150	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.140.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.50.141.152	147.237.0.16	United Arab Emirates	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
198.180.198.185	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1

03-06-2016-12:04:02 to 03-06-2016-13:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.136.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
2.52.43.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.238	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
2.52.140.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.180.119.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
176.13.22.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.130.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
87.71.35.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.52.43.27	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
109.64.115.162	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.32.179.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.18.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.218	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
194.90.107.12	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.44.40	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.148.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	9
2.54.38.64	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.117.182.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.52.43.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.52.43.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.43.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
109.253.129.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.24.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.210.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.108.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.33		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.55.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.55.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.43.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.80.102.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
180.191.115.29	Philippines	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.55.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.43.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.43.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.43.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
192.116.175.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
2.54.38.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.52.40.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.52.167.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.14.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
103.40.163.112		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.40.163.112	Block	26
80.246.136.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
2.52.43.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.18.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.52.24.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.129.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.189.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.35.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.48.86	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/sip_storage/files/7/1887.pdf&sa=u&ved=0ahukewibza7g66vlahvdmbokhy3od6eqfggpmai&usg=afqjcnf515tzl0xbus5txyeabmkzbgecfq	Block	2
70.39.157.199	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.148.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
103.40.163.112		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	2
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.22.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.111.139.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
31.168.147.203	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
85.114.127.49	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.222	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
193.227.19.122	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.22.131.24	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
79.177.81.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
66.249.66.182	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/webresource.axd	Block	1
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
197.33.15.19	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
87.70.6.192	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
37.26.146.193	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.130.118.60	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.152.146	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /x	Block	1
103.40.163.112		147.237.77.216	dover.idf.il	Admin Blocking	Block	1
46.63.216.184	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
85.250.75.35	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
37.142.68.100	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
193.227.19.122	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
5.22.131.24	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.180.119.111	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
103.40.163.112		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
66.249.66.185	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1