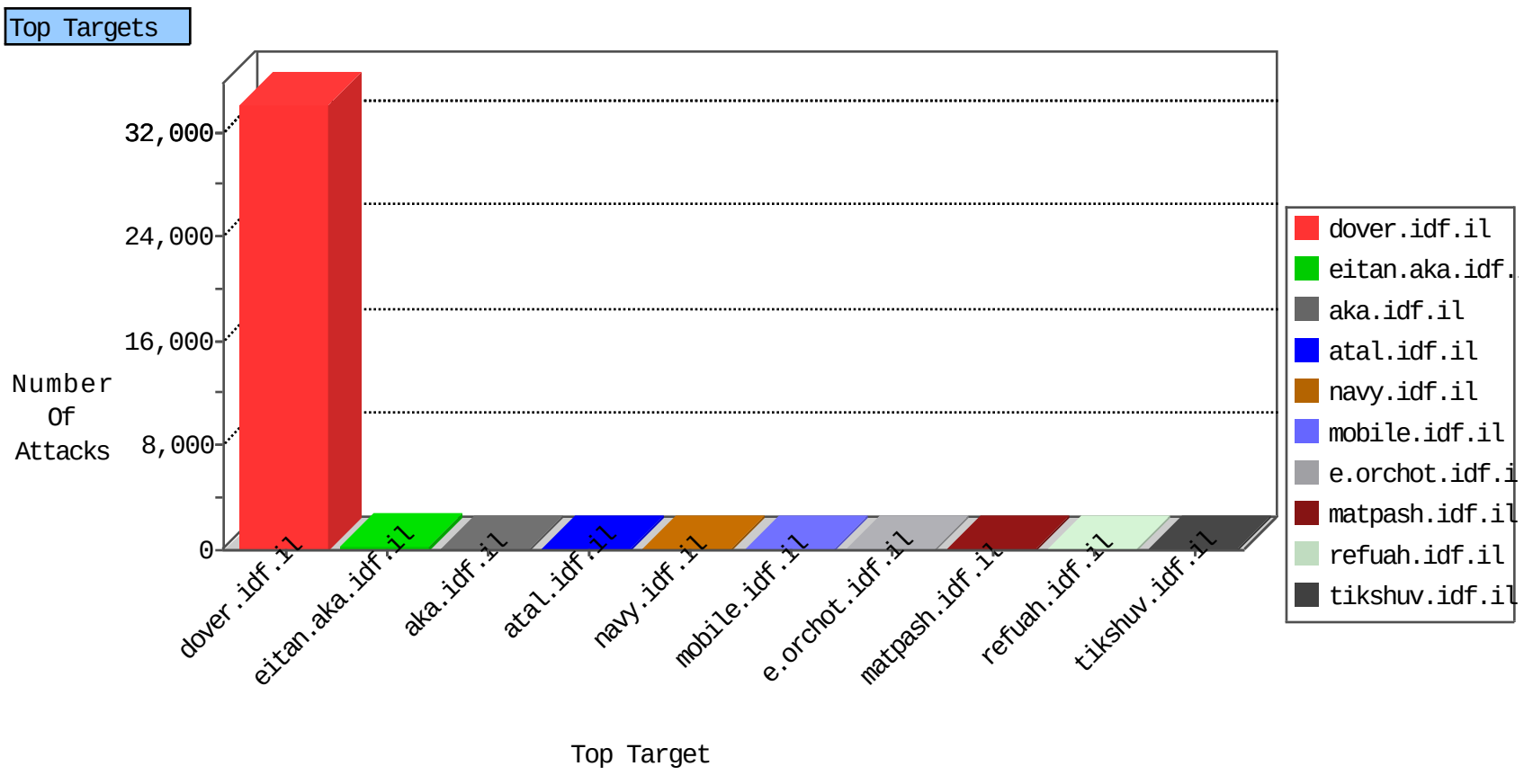
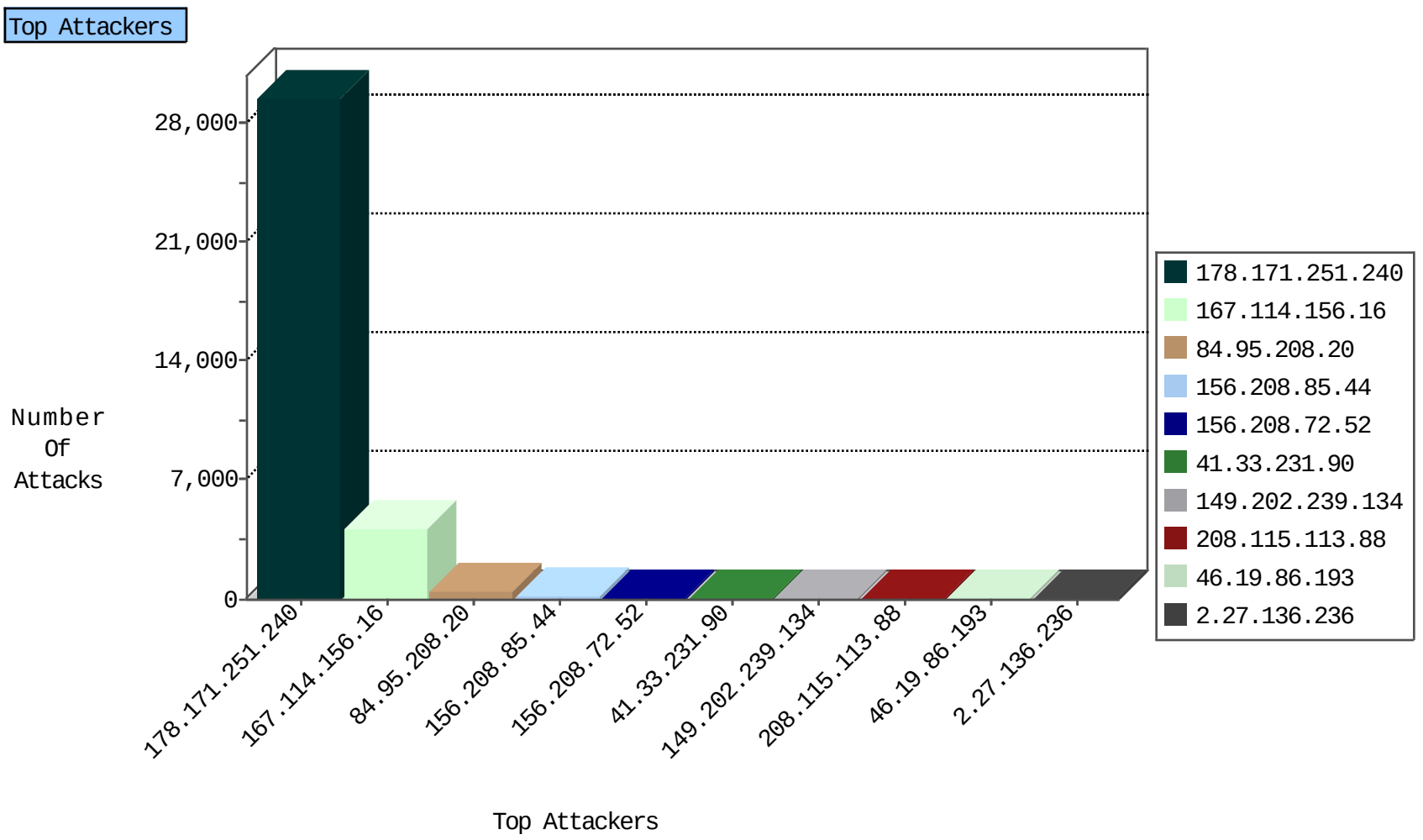
04-17-2016-03:04:06 to 04-17-2016-04:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-17-2016-03:04:06 to 04-17-2016-04:04:06

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	4117
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	113
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	20
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	2
82.145.231.154	Turkey	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
179.43.141.194	Switzerland	147.237.0.19	madim.atal.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
179.43.141.194	Switzerland	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

04-17-2016-03:04:06 to 04-17-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-17-2016-03:04:06 to 04-17-2016-04:04:06

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
191.32.181.8	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.93.137.14	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.235.254.181	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
95.9.65.77	147.237.8.24	Turkey	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
84.200.15.174	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.142.238	147.237.8.14	France	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.104	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.130	147.237.0.15	Romania	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
106.186.113.67	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
95.9.65.77	147.237.8.24	Turkey	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.76.197	Germany	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

04-17-2016-03:04:06 to 04-17-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	22115
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4443
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2740
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	144
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack		reject	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
46.19.86.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.27.136.236	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
54.193.101.12	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
77.126.196.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.16.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.140	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
2.27.136.236	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
157.55.39.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
199.30.72.92	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.204	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
97.94.241.237	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.210.142.238	France	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.196	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
199.30.72.92	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.180.28.83	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.57.0.199	Mexico	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.205	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.32.179.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.210.142.238	France	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.197	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.210.142.238	France	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.199	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.90.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
62.210.142.238	France	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	98
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	6
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	6
199.30.24.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.45	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.16.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
157.55.39.163	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.163	Block	3
199.30.24.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	2
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	2
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69051.pdf	Block	1
157.55.39.163	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.163	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2975.jpg	Block	1
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.172	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
157.55.39.163	United States	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 157.55.39.163	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/general.aspx	None	1
128.232.110.28	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
157.55.39.163	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.86.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
199.47.81.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497-	Block	1
157.55.39.41	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
81.111.195.163	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3249.jpg	Block	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.136	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
81.111.195.163	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
65.55.210.137	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1

04-17-2016-03:04:06 to 04-17-2016-04:04:06