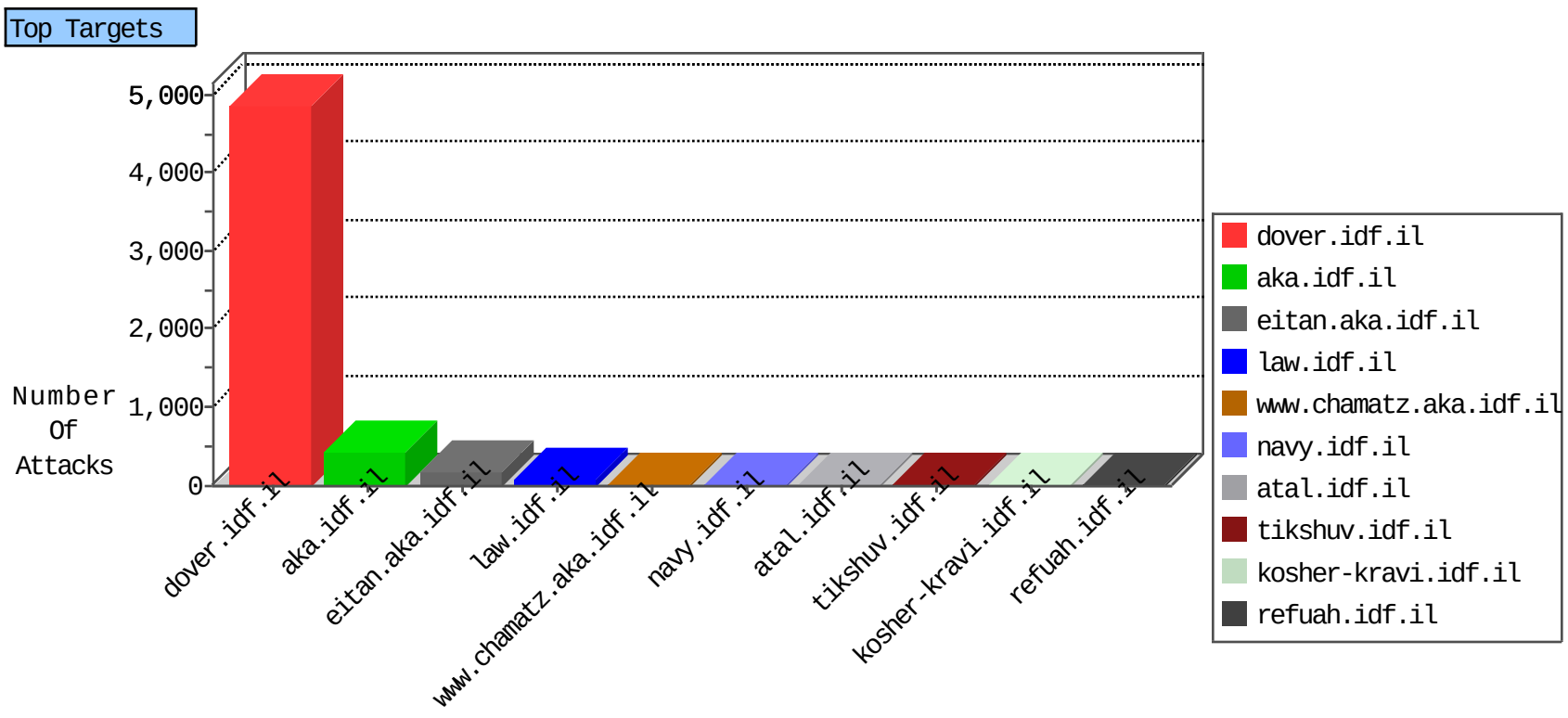
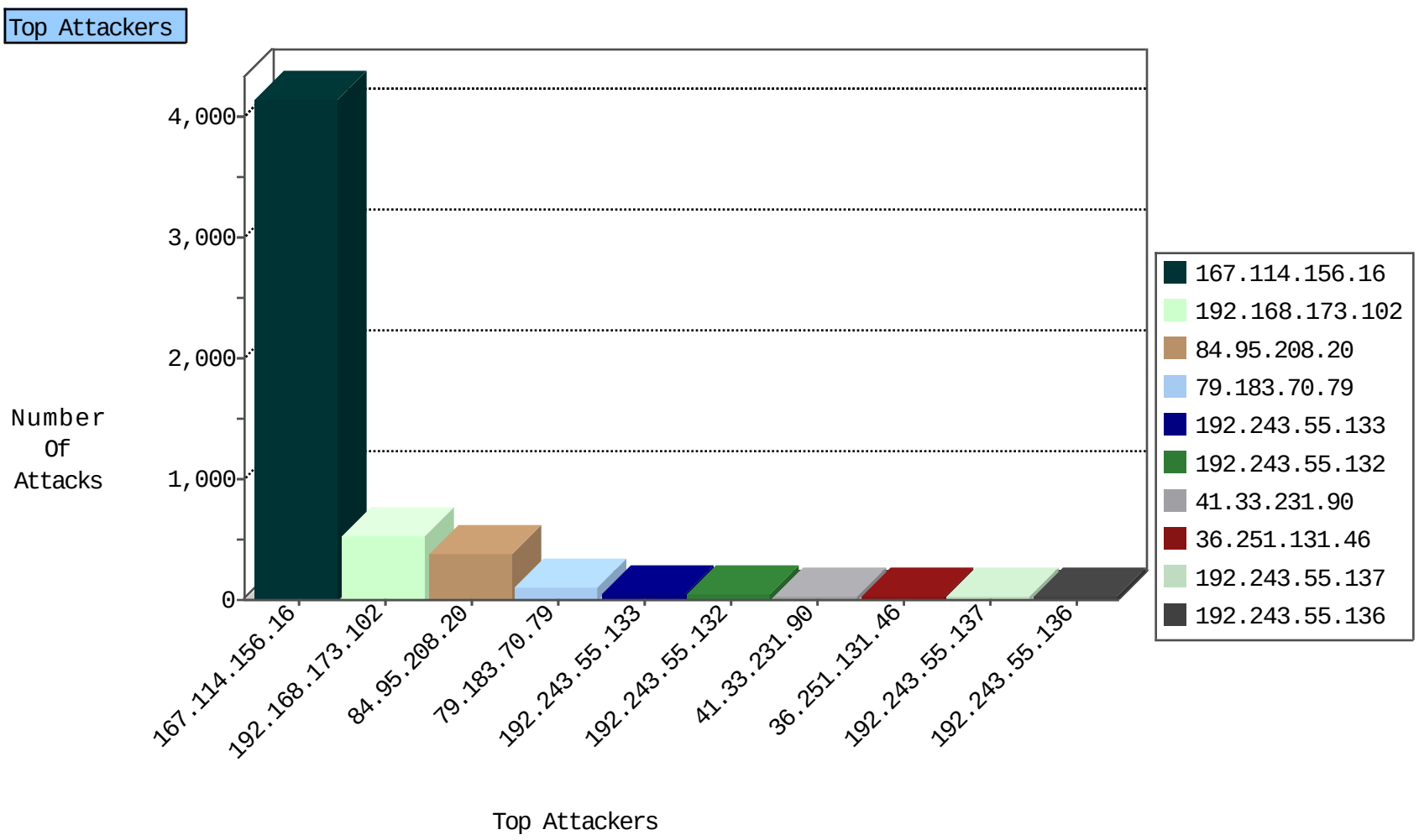
04-11-2016-02:04:09 to 04-11-2016-03:04:09

IDF Under Attack Daily Report





04-11-2016-02:04:09 to 04-11-2016-03:04:09

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	4157
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
176.31.60.249	France	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1
219.232.243.28	China	147.237.8.50	e.tikshuv.idf.il	Invalid TCP Flags	drop	1
115.159.150.148	China	147.237.72.14	dover.idf.il(old)	L4 Source or Dest Port Zero	drop	1
179.43.144.50	Switzerland	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
110.76.40.33	China	147.237.8.45	e.eitan.idf.il	L4 Source or Dest Port Zero	drop	1
219.232.243.28	China	147.237.77.74	law.idf.il	Invalid L4 Header Length	drop	1
219.232.243.28	China	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
110.76.40.33	China	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	1
174.37.194.144	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
81.169.254.70	Germany	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
219.232.243.28	China	147.237.0.35	akaws.idf.il	Invalid L4 Header Length	drop	1
110.76.40.33	China	147.237.76.44	e.refuah.idf.il	Invalid TCP Flags	drop	1

04-11-2016-02:04:09 to 04-11-2016-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.122	China	147.237.76.31	nakchal.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	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-02:04:09 to 04-11-2016-03:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
174.37.194.144	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
89.16.84.104	147.237.8.14	Ireland	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
76.181.249.213	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
211.149.156.87	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.94	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
89.16.84.104	147.237.8.14	Ireland	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
76.181.249.213	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
195.216.176.244	147.237.77.170	Latvia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
54.218.50.136	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

04-11-2016-02:04:09 to 04-11-2016-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	350
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	188
79.183.70.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
36.251.131.46	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
207.46.13.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.131	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
156.207.7.229	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.126.93.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.233.58	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.189.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.58.64	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.13.11.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
156.207.7.229	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.71.1.176	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.133	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.132	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

04-11-2016-02:04:09 to 04-11-2016-03:04:09

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	119
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
36.251.131.46	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.251.131.46	Block	22
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	18
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	11
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	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
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
36.251.131.46	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1497-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
47.88.34.12	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58625&docid=68481	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390&docid=57273	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
177.98.5.225	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
94.199.151.22	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62669&docid=77953	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
47.88.34.12	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/include/vdimgck.php	Block	1
199.30.24.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.184.238.200	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
177.98.5.225	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/xxu.php	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
65.55.210.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.129	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /x	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
36.251.131.46	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1515-en/contact.php	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59269&docid=59486	Block	1
159.203.162.199	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1

04-11-2016-02:04:09 to 04-11-2016-03:04:09