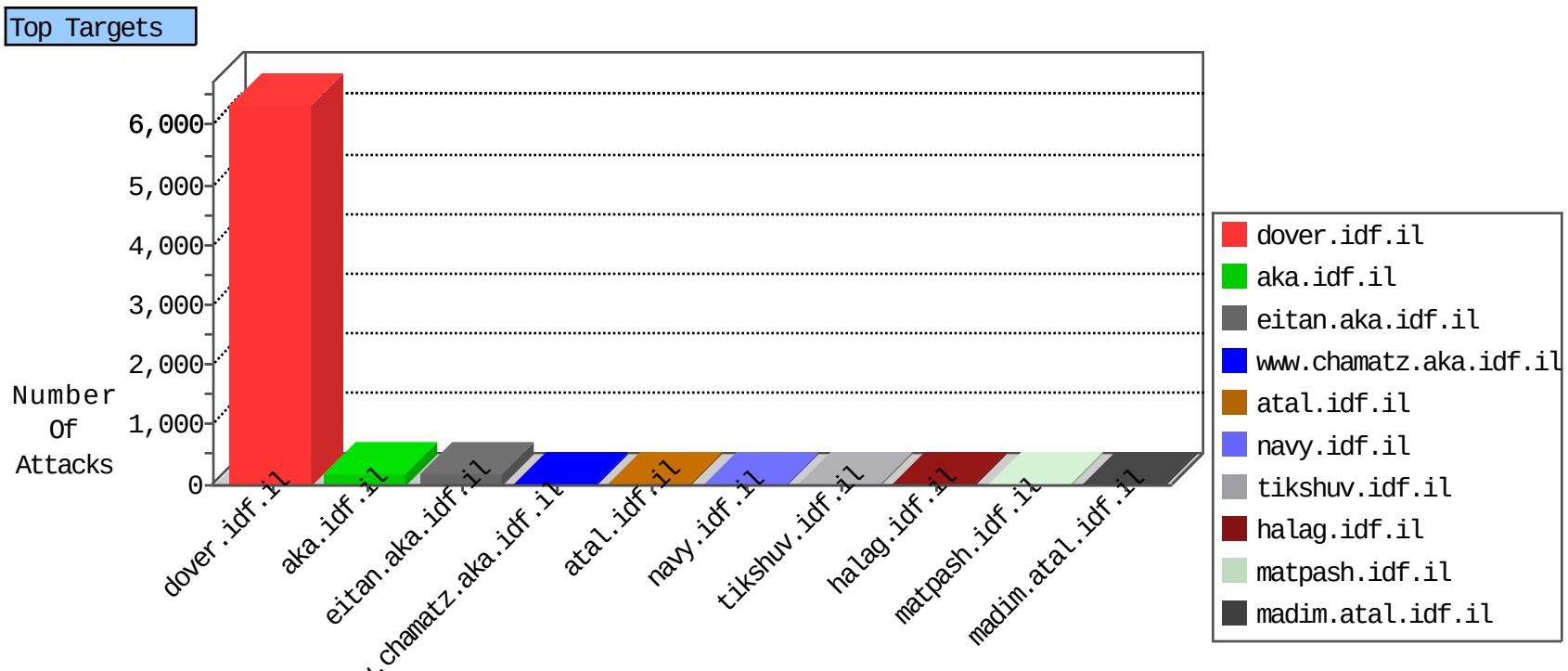
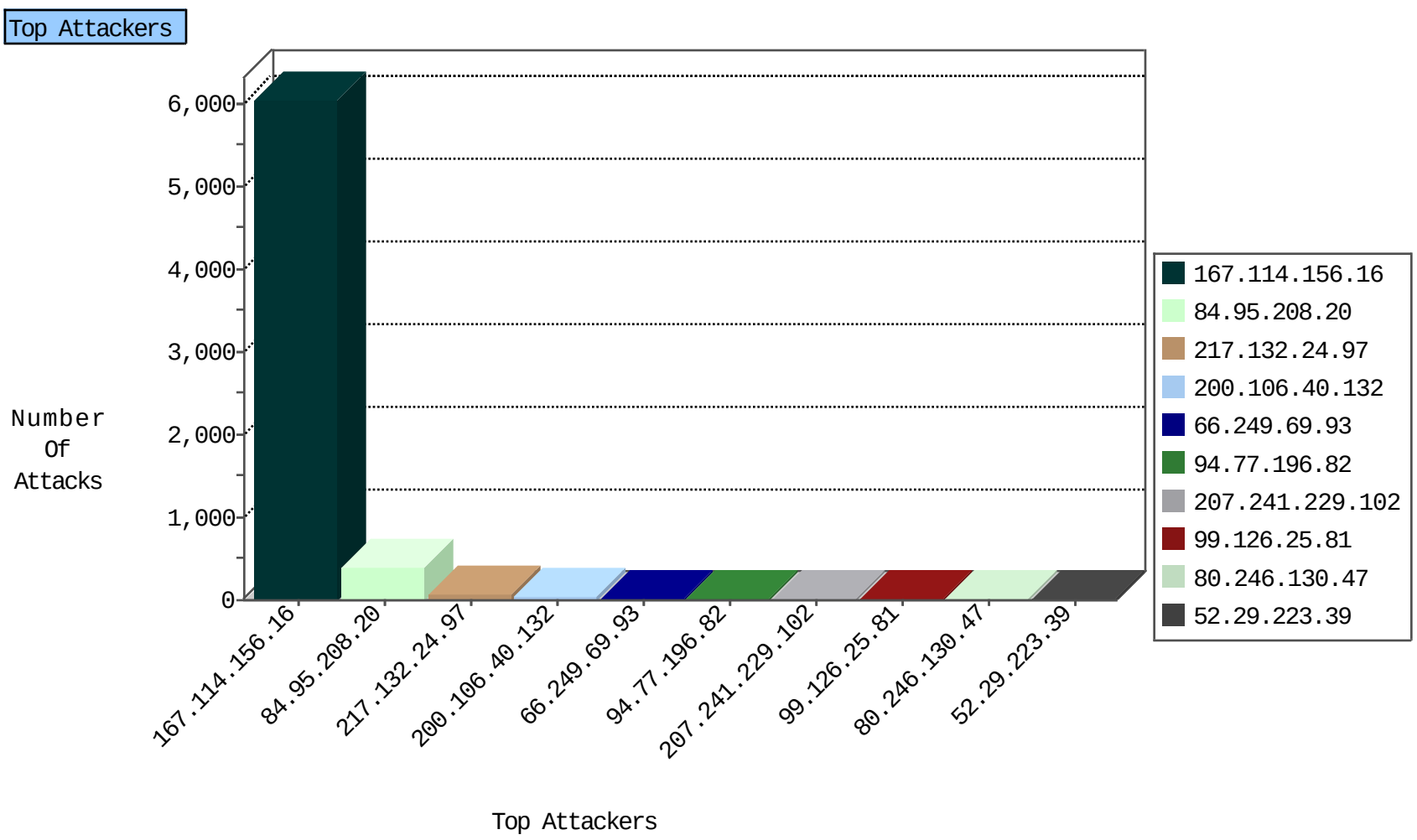
04-21-2016-02:04:09 to 04-21-2016-03:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-21-2016-02:04:09 to 04-21-2016-03:04:09

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	HTTP-POST-Segmented-DoS	dest-reset	11470
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1250
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	401
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
109.186.49.99	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1
85.65.88.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1
89.248.160.138	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
69.30.226.222	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
94.102.52.10	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1

04-21-2016-02:04:09 to 04-21-2016-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-02:04:09 to 04-21-2016-03:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.47	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
107.158.255.194	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
107.158.255.194	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1
93.180.66.29	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
93.180.66.29	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.99	147.237.76.200	Lithuania	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.99	147.237.76.197	Lithuania	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.99	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.0.16	Lithuania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
65.181.123.161	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.220.135	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
106.120.173.154	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
93.180.66.29	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.99	147.237.77.243	Lithuania	mobile.idf.il	ET SCAN Potential SSH Scan	1
93.180.66.29	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.99	147.237.76.199	Lithuania	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.99	147.237.76.39	Lithuania	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.200	Lithuania	m4u.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.0.15	Lithuania	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
65.181.123.161	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-21-2016-02:04:09 to 04-21-2016-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5336
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
217.132.24.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
200.106.40.132	Peru	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
99.126.25.81	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
65.92.15.153	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.227.67.169	Sweden	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.68.125	Israel	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
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
99.126.25.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
99.126.25.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.29.67.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
118.173.129.184	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
85.130.251.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.246.130.47	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.28.115.230	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.64.92.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.119.124.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.59.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
128.232.110.28	United Kingdom	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.53.59.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
193.92.20.250	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.59.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.53.59.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
217.132.24.97	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
2.53.59.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.223	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.28	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1

04-21-2016-02:04:09 to 04-21-2016-03:04:09

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	118
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	75
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	28
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed 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
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
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	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
157.55.39.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
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	147.237.0.34	tikshuv.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	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	1
207.46.13.62	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
149.78.37.96	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	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
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
217.132.24.97	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1093-he/eitan.aspx	None	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
157.55.39.223	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
217.132.24.97	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	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
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/login.aspx?moduletogoto=0	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
77.75.77.32	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/35/	Block	1
194.28.115.230	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
106.120.173.154	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.29.140.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
83.130.106.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
194.28.115.230	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
149.78.37.96	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
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	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed 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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1

04-21-2016-02:04:09 to 04-21-2016-03:04:09