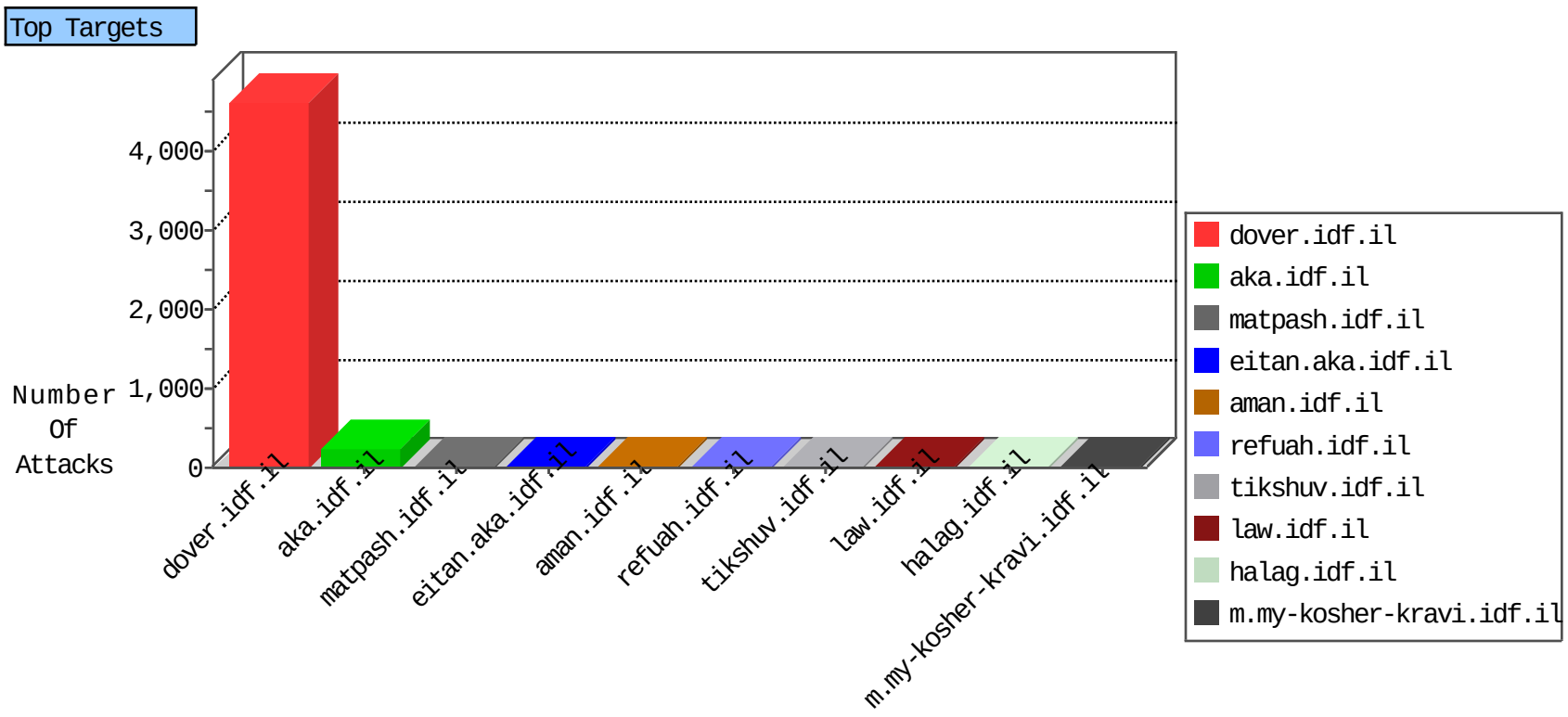
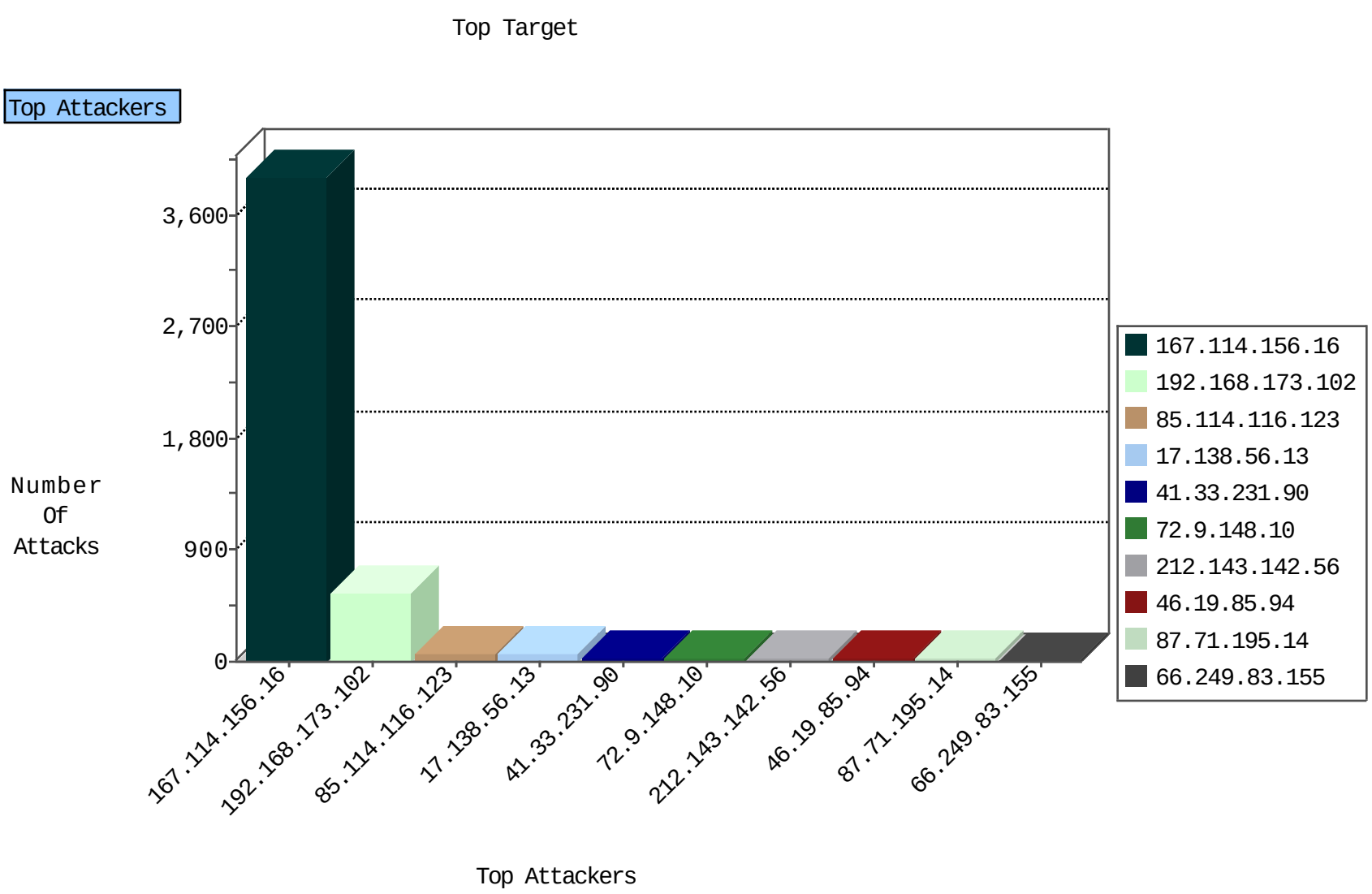
04-09-2016-01:05:18 to 04-09-2016-02:05:18

IDF Under Attack Daily Report





04-09-2016-01:05:18 to 04-09-2016-02:05:18

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15165
46.19.85.94	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7301
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3911
128.177.133.102	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3591
85.114.116.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2903
66.249.83.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1424
144.76.4.148	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1102
46.19.85.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	772
72.9.148.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	200
82.166.171.208	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	80
85.114.116.123	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	69
185.120.125.41	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	2
209.126.127.17	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
105.91.213.208	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.61.137.66	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
17.138.56.13	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.127.17	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
197.116.186.233	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.127.17	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1

04-09-2016-01:05:18 to 04-09-2016-02:05:18

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
77.125.2.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.99.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
144.76.4.148	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

04-09-2016-01:05:18 to 04-09-2016-02:05:18

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
59.45.79.103	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
52.34.151.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
52.34.151.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.199.172.154	147.237.76.39	Lithuania	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
93.183.201.2	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
52.34.151.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.199.172.154	147.237.76.39	Lithuania	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
105.91.213.208	147.237.77.216	Egypt	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
65.98.40.74	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-09-2016-01:05:18 to 04-09-2016-02:05:18

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	360
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	197
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
87.71.195.14	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
147.236.32.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
45.59.183.149	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.114.116.123	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
149.78.26.209	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.83.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.199.186.15	Denmark	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.3.147.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.41.196	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.104.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
123.126.113.109	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
46.19.86.223	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.144.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
5.28.173.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.111.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.178.224.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.203.136.75	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
109.64.136.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.213.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop		drop	2
84.108.246.13	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
105.91.213.208	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.24.197	United States	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.62.195	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.142.236.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.148.44.148	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.246.13	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.212	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illega start line in request	monitor	1
106.186.113.132	Japan	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
217.78.141.141	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.11.180.67	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

04-09-2016-01:05:18 to 04-09-2016-02:05:18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.211.228.121	Qatar	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	5
37.211.228.121	Qatar	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	4
37.211.228.121	Qatar	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	3
169.229.3.90	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/ts.php	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
207.46.13.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.94	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
207.46.13.105	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
157.55.39.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.94	Block	1
31.6.38.194	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
178.214.94.131	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.94	Block	1
31.44.128.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
197.116.186.233	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
79.176.96.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...37&docid=68534	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_id.20.8afc=4220bc9769a9810e.1460156389.1.1460156389.1460156389.; _pk_ses.20.8afc=*	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method L,he;q=0.8,en-US;q=0.6,en;q=0.4 in URL	Block	1
204.79.180.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1

04-09-2016-01:05:18 to 04-09-2016-02:05:18