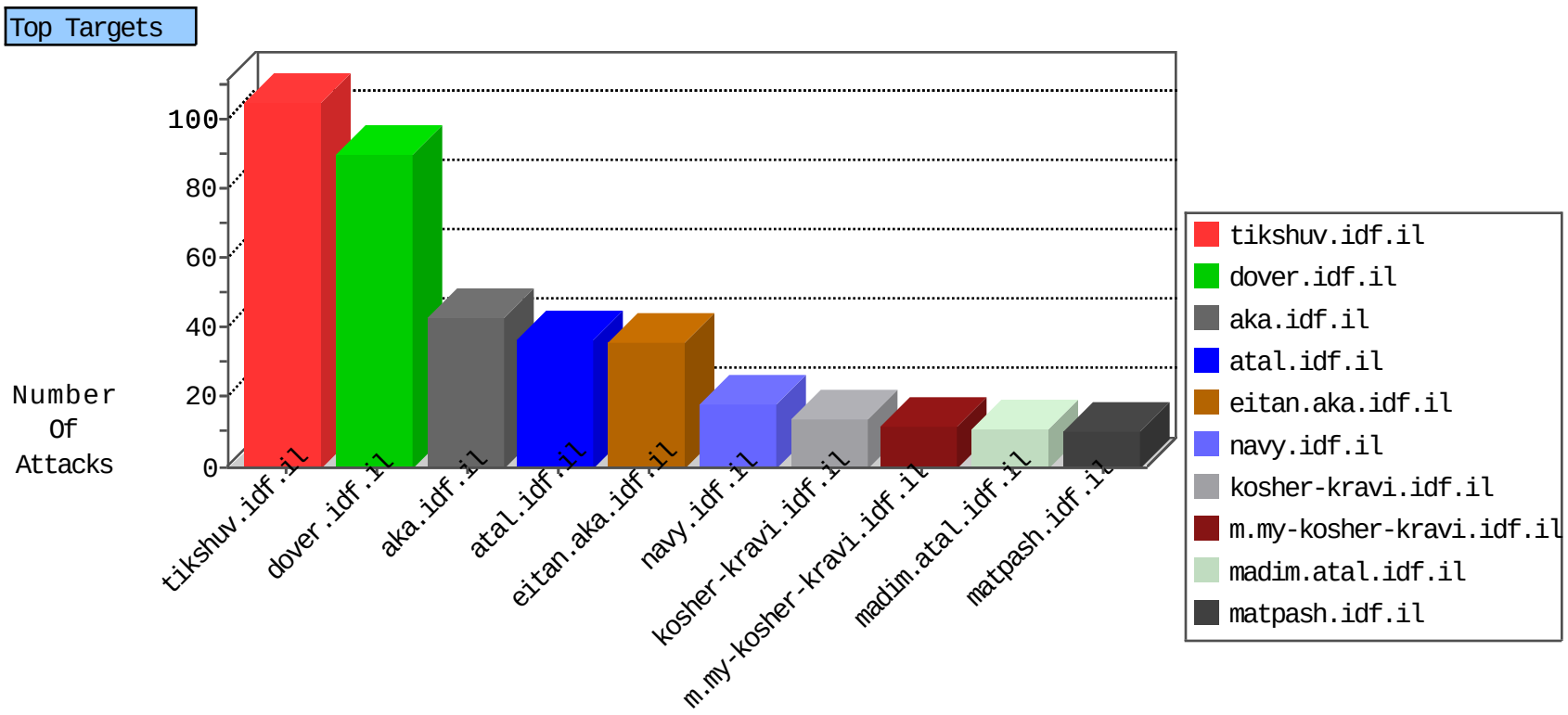
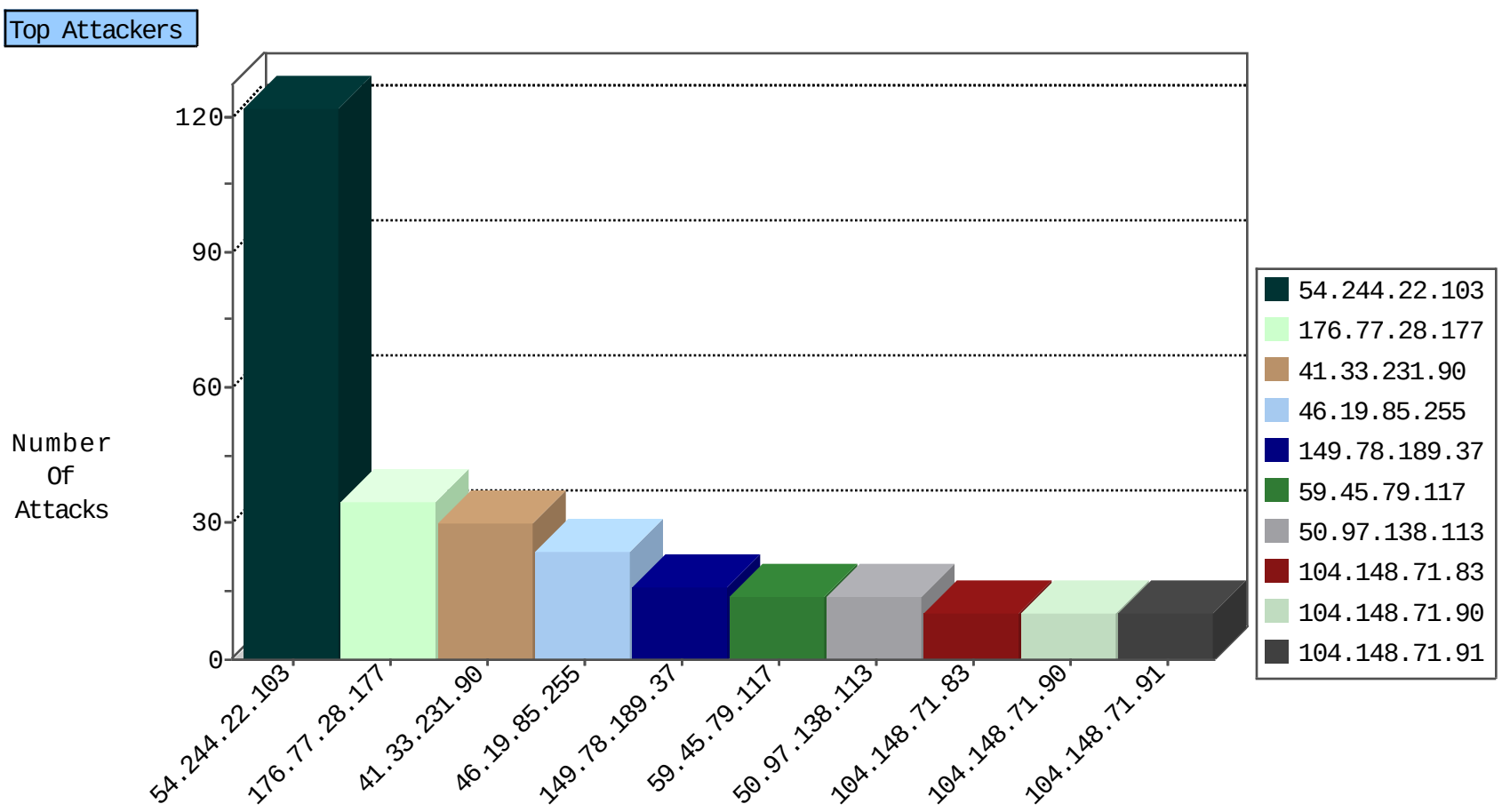
02-20-2016-01:04:14 to 02-20-2016-02:04:14

IDF Under Attack Daily Report



Top Target



Top Attackers

02-20-2016-01:04:14 to 02-20-2016-02:04:14

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
183.60.48.25	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
211.200.214.69	Korea, Republic of	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
27.221.10.194	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.130.5.200		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
211.200.214.69	Korea, Republic of	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
45.32.57.134		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.200		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
45.32.57.134		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

02-20-2016-01:04:14 to 02-20-2016-02:04:14

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
38.87.46.138	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
157.55.39.41	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
80.235.155.54	United Kingdom	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-20-2016-01:04:14 to 02-20-2016-02:04:14

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
120.24.72.25	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
222.124.152.67	147.237.76.202	Indonesia	e.halag.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
95.154.184.100	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.63.158	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
173.14.248.34	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
121.147.228.26	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
222.124.152.67	147.237.76.177	Indonesia	ncore.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.98	147.237.77.205	United States	prisha.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
95.154.184.100	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
173.14.248.34	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

02-20-2016-01:04:14 to 02-20-2016-02:04:14

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	85
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	37
176.77.28.177	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
50.97.138.113	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
104.148.71.83	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
104.148.71.90	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
104.148.71.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.54.172.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.255	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
120.52.72.47	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.255	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.218	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.22.130.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.28.160.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.205.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.235.155.54	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.235.155.54	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.9.111.70	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
77.237.138.202	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.175	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.140.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
185.3.144.68	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
120.52.72.43	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
82.166.100.163	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.175	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.94.33.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
161.202.72.162	Netherlands	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.13.40.120	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.174	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.237.234.64	Slovakia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.210.181.15	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
161.202.72.162	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.97.138.113	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
141.212.122.174	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.180.64.220	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
109.73.127.69	United Kingdom	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

02-20-2016-01:04:14 to 02-20-2016-02:04:14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.189.37	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.189.37	Block	15
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	4
197.38.225.107	Egypt	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	2
197.38.225.107	Egypt	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	2
37.238.144.116	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.238.144.116	Block	2
149.78.189.37	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
50.97.138.113	United States	147.237.72.166	aka.idf.il	Multiple signatures from 50.97.138.113	Block	1
207.46.13.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
89.39.93.218	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
37.238.144.116	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22787ayedar/dover.aspx	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
95.73.241.125	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
41.202.219.72	Cameroon	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.12.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19825-he/dover.aspx	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
103.18.118.6	New Zealand	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
41.202.219.72	Cameroon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
80.246.130.3	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.69.133.246	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/kurs/default.asp	Block	1
141.212.122.160	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
50.97.138.113	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
89.39.93.218	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1

02-20-2016-01:04:14 to 02-20-2016-02:04:14