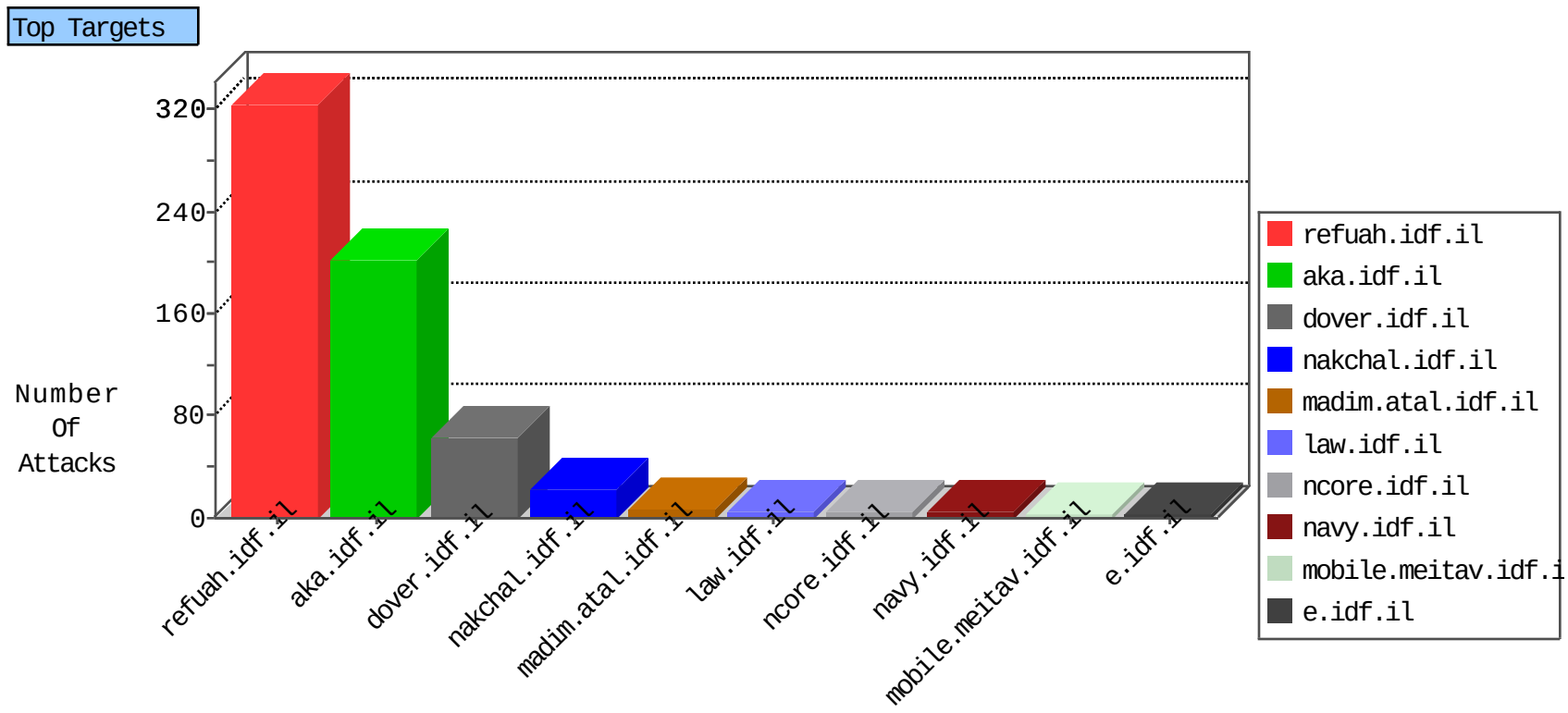
09-20-2016-05:04:06 to 09-20-2016-06:04:06

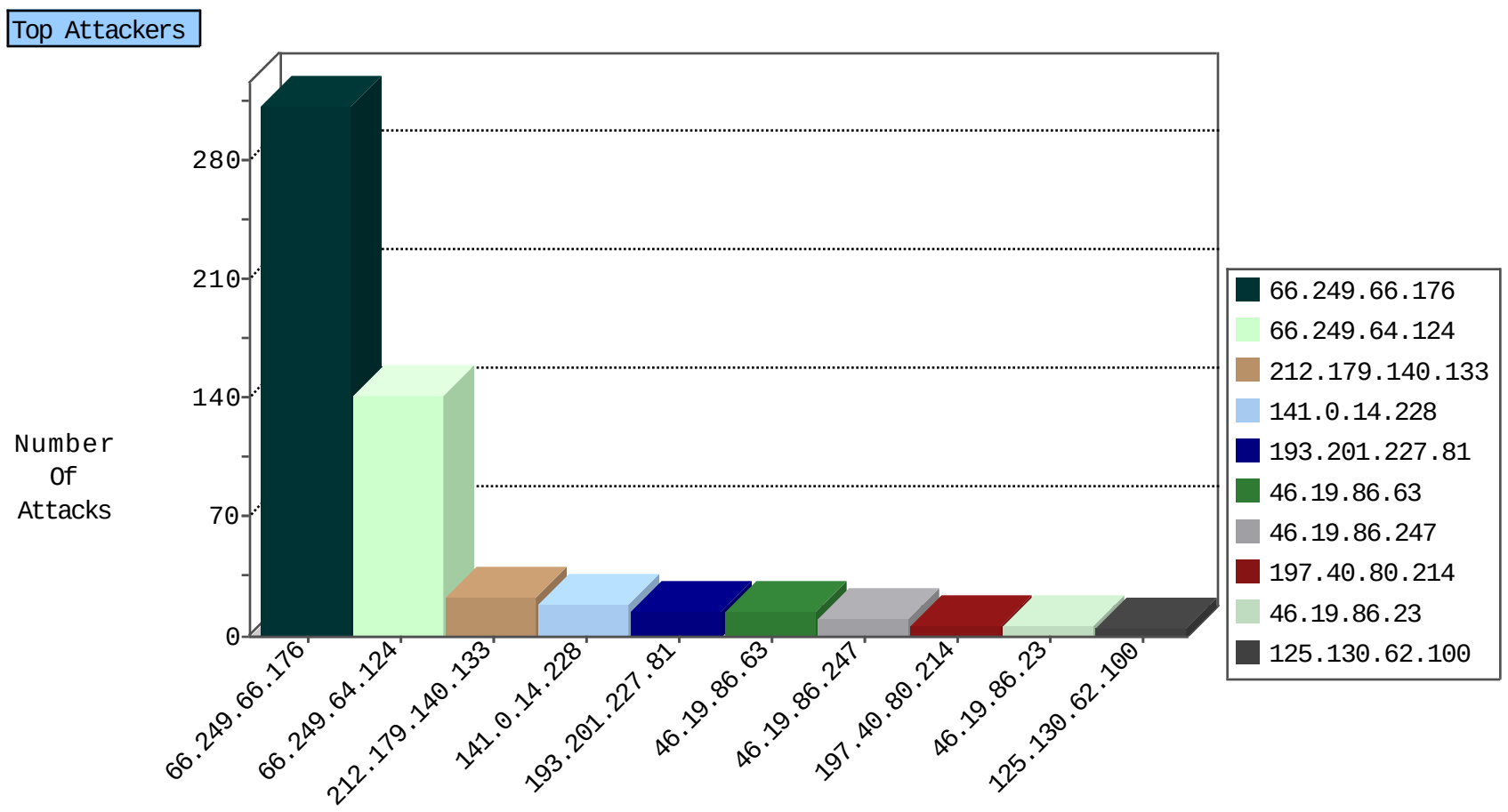
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-20-2016-05:04:06 to 09-20-2016-06:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.62.53.168	Russian Federation	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.201.227.81	Ukraine	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-20-2016-05:04:06 to 09-20-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-20-2016-05:04:06 to 09-20-2016-06:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.176	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	312
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	142
193.201.227.81	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential SSH Scan	2
193.201.227.81	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.99	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
125.130.62.100	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
200.6.65.102	147.237.8.45	Chile	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
24.173.213.138	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
125.213.243.10	147.237.0.17	Thailand	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.130.62.100	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN Potential SSH Scan	1
125.130.62.100	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.214.107.200	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.63.246.42	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.72.156	Ukraine	aman.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.160.222.18	147.237.0.34	South Africa	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
125.213.243.10	147.237.0.35	Thailand	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
200.6.65.102	147.237.8.27	Chile	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
125.130.62.100	147.237.0.200	Korea, Republic of	m4u.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN Potential SSH Scan	1
122.54.135.121	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.227.81	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
69.162.69.222	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.81	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
193.201.227.81	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.4.85.112	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

09-20-2016-05:04:06 to 09-20-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.179.140.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
141.0.14.228	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.23	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.128.113	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
177.23.224.11	Brazil	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
68.180.229.223	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
197.40.80.214	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.113.155	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.63	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
197.40.80.214	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
138.246.253.19	Germany	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.63.246.42	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1
46.4.85.112	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
197.40.80.214	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
138.246.253.19	Germany	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
75.76.248.31	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	1
46.4.85.112	Germany	147.237.0.33	idf.il	drop		drop	1
108.184.188.229	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
69.162.69.222	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.86.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
199.241.27.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.4.85.112	Germany	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
197.40.80.214	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.64.111.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.237.154	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.62	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
197.40.80.214	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
123.125.71.84	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.63.246.42	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

09-20-2016-05:04:06 to 09-20-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.27.83	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method .; in URL _pk_ses.119.2366=*	Block	1
5.3.236.34	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
195.62.53.168	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
46.19.86.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
40.77.167.73	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
213.57.13.153	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
73.165.154.36	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$txtSearch in www.idf.il/1283-en/dover.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1
217.69.133.247	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
73.188.157.161	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
91.108.178.210	Sweden	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
46.19.86.63	Israel	147.237.76.31	nakchal.idf.il	Malformed URL _pk_ses.119.2366=*	Block	1
91.108.178.210	Sweden	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/wp/wp-login.php	Block	1

09-20-2016-05:04:06 to 09-20-2016-06:04:06