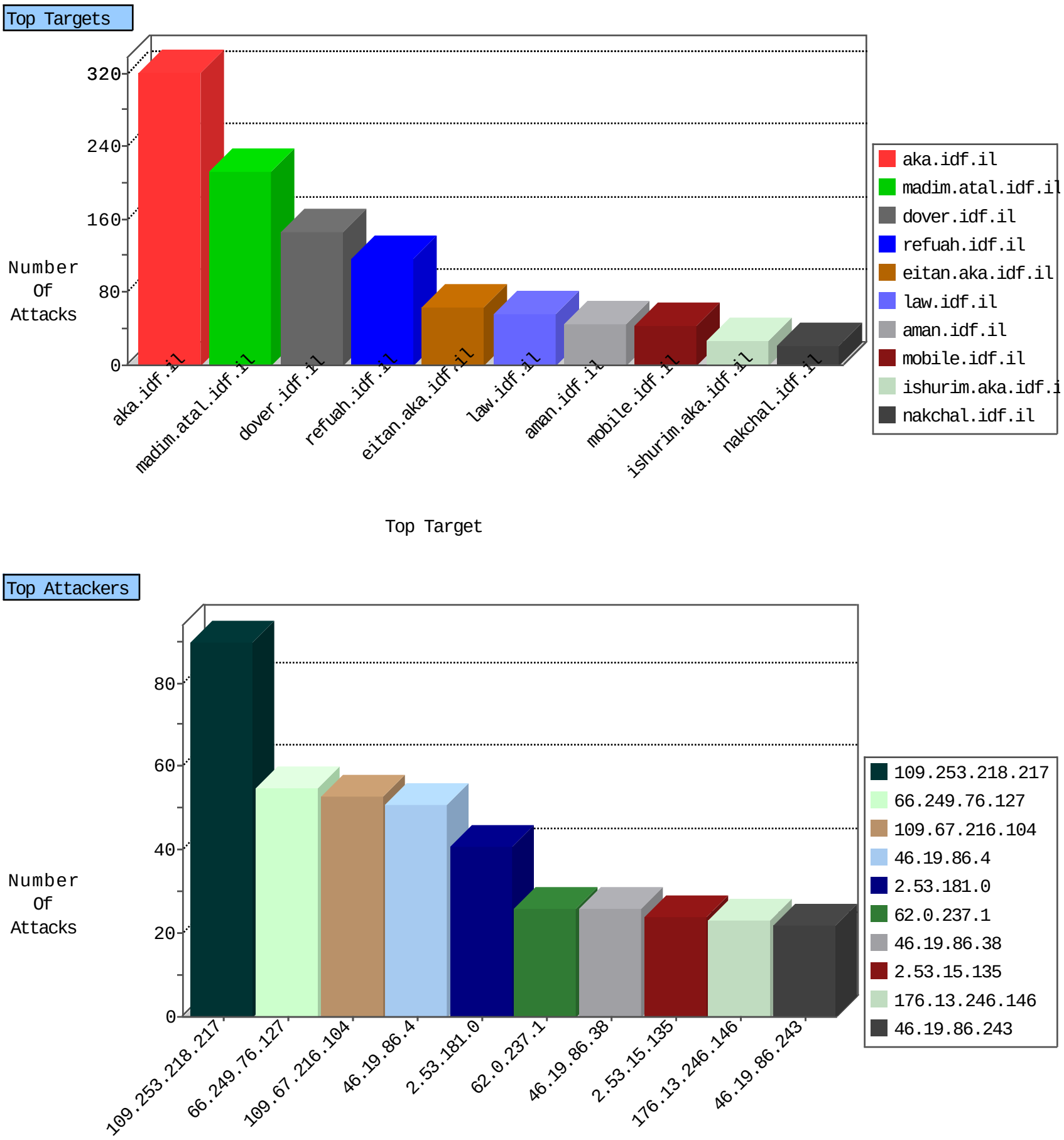
09-14-2016-11:04:08 to 09-14-2016-12:04:08

IDF Under Attack
Daily Report



09-14-2016-11:04:08 to 09-14-2016-12:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.238.138.252	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1179
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	39
109.65.125.134	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.194.252.9	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	3
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	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
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.117.226.180	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.19.86.161	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.14	dover.idf.il(old)	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
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-11:04:08 to 09-14-2016-12:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-14-2016-11:04:08 to 09-14-2016-12:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	55
82.80.166.173	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
82.80.193.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.168.208	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.3.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.238.138.252	147.237.77.216	Iraq	dover.idf.il	ET SCAN NMAP -sS window 1024	1
192.117.142.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.107.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.49.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.55.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.87.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.109.43.252	147.237.77.226	Colombia	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.159.254.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-14-2016-11:04:08 to 09-14-2016-12:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.216.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	41
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
2.53.15.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
62.0.232.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
100.92.245.169		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.26.149.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.85.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
62.0.225.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
62.0.224.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
106.120.188.69	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
80.246.130.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.18.195	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.229.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.154.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
37.26.146.220	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.138.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.70	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
194.90.25.122	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.220	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.3.147.84	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.138.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.8.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.116.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.55.60.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.170.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-14-2016-11:04:08 to 09-14-2016-12:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.218.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.53.181.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.246.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
109.67.216.104	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	10
77.139.168.208	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
192.115.252.2	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
195.160.242.40	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
89.138.169.40	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
195.160.242.40	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.115.252.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
176.13.20.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.29.204.108	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.191.157	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
77.124.3.123	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1122-he/nakhal.aspx	Block	2
80.246.137.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19667-he/idfgdover.aspx)	Block	1
109.67.216.104	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
37.26.146.215	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.117.105.117	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 3	Block	1
77.139.168.208	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
54.196.104.181	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
157.55.39.56	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/smalim/faq.aspx	Block	1
89.139.164.174	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.117.105.117	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]E5½l'*[[#7]]*[[#25]]å[[#15]]µúJ•ÅŒ&_,GµD{'•¾â[[#15]][[#3]][[#30]]Ì in URL q[[#25]]ענ"פ[[#21]]x¸¨ˆ.-ß[[#24]]}[[ע#12ˆj]]'xa:¸]]02#[[¸/¸]]91#[[·¨·]]81#[[]]0#[[t]]6#[[sž)[[#19]][[#0]]œ[[#0]]5[[#0]]/[[#0]]	Block	1
80.230.229.19	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.117.105.117	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name ôk•	Block	1
185.27.106.239	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
204.79.180.63	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
109.253.198.106	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.117.105.117	Israel	147.237.77.216	dover.idf.il	Malformed URL q[[#25]][[ענ"פ#21}]]42#[[ß-¸ˆ¨¸x]]ע[[21#]]jˆ':ax œ)žs[[#6]]t[[#0]][[#18]]·¨·[[#19]]¸/¸[[#20]]¸[[#19]][[#0]]œ[[#0]]5[[#0]]/[[#0]]	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/home.png	Block	1
77.139.168.208	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/accepted.aspx	Block	1
192.115.252.2	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.115.252.2	Block	1
66.249.64.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
159.203.91.110	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for list.ips.gov.il/	Block	1
109.67.181.214	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
5.29.204.108	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 5.29.204.108	Block	1
193.5.216.100	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
192.117.105.117	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]E5½l'*[[#7]]*[[#25]]å[[#15]]µúJ•ÅŒ&_,GµD{'•¾â[[#15]][[#3]][[#30]]Ì	Block	1
80.246.130.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.27.106.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
204.79.180.218	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
192.117.105.117	Israel	147.237.77.216	dover.idf.il	NULL Character in Header Name at o0[[#11]][[#15]]-[[#11]]¥v®#Ùj.ÎÏ«[[#31]]s±Hv[[#26]]˜K•F[[#25]]3·øH€WÑä¿[[#31]]ýŠiúÚ•	Block	1

09-14-2016-11:04:08 to 09-14-2016-12:04:08