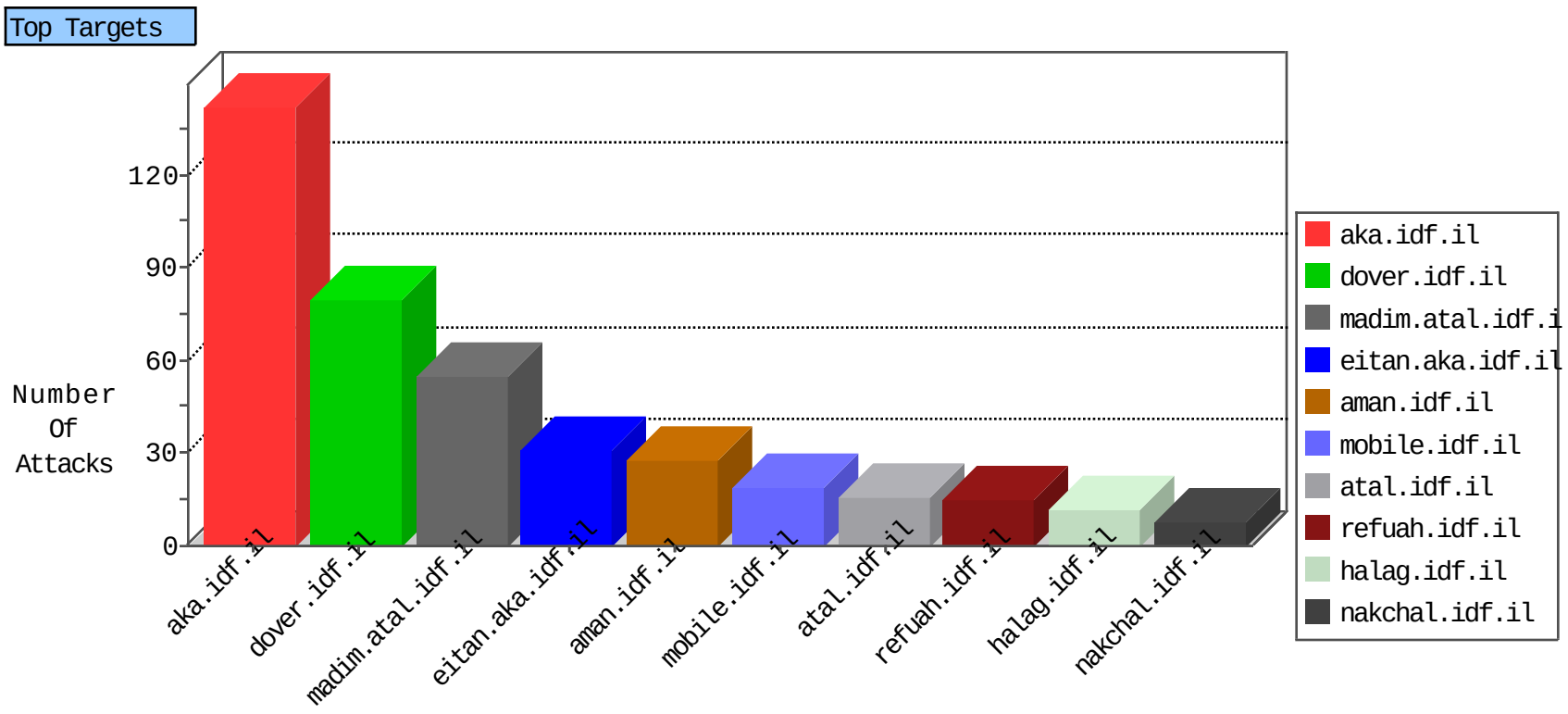
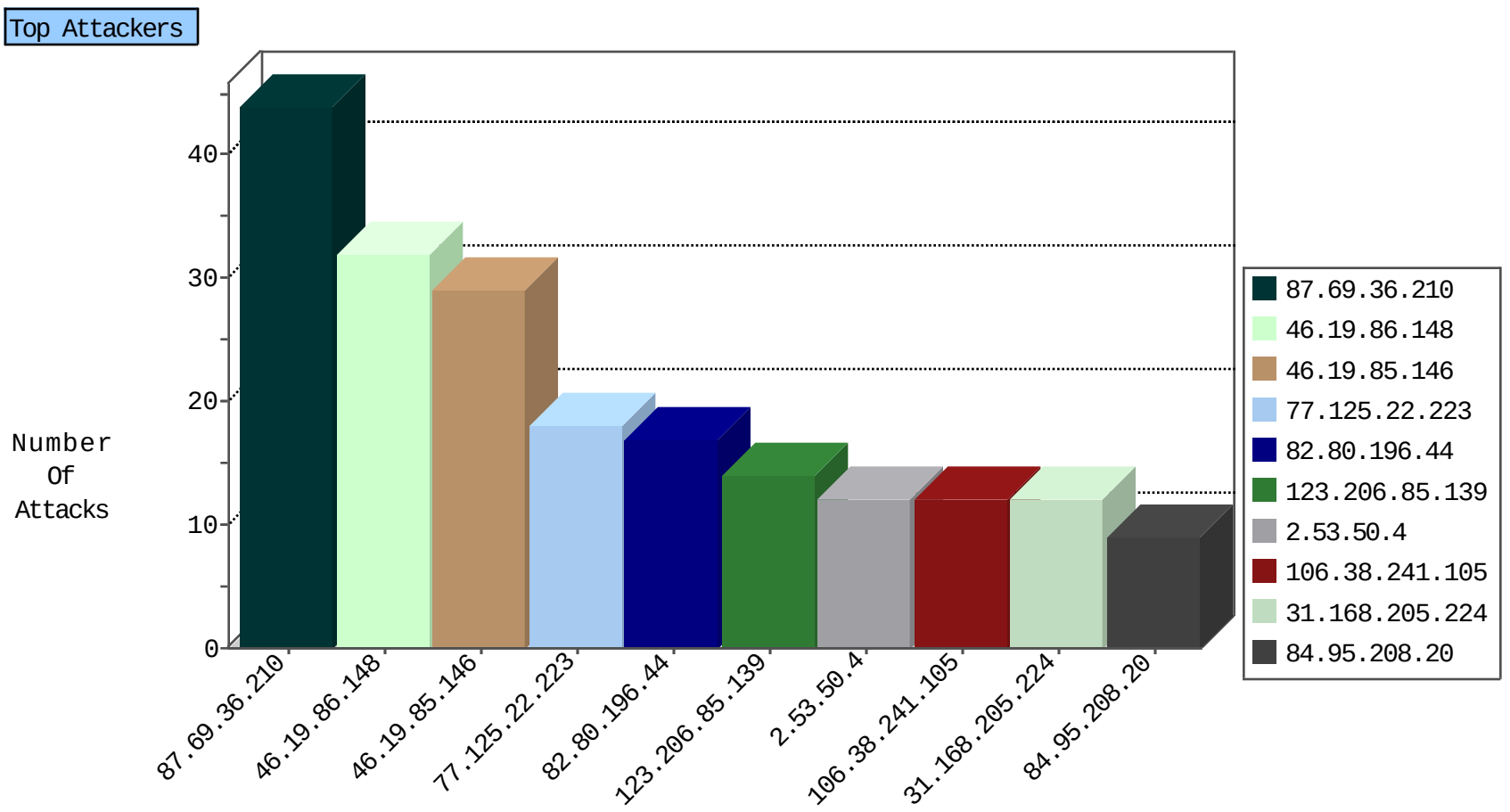
09-16-2016-10:04:06 to 09-16-2016-11:04:06

IDF Under Attack Daily Report





09-16-2016-10:04:06 to 09-16-2016-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
198.204.224.237	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.252	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
208.110.84.69	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
195.113.161.84	Czech Republic	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
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
63.141.231.194	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
173.208.150.117	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.110.84.69	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
63.141.242.195	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
198.204.224.235	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
142.54.174.85	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
69.30.193.251	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
208.110.84.66	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-10:04:06 to 09-16-2016-11:04:06

Top Attackers In IPS

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

09-16-2016-10:04:06 to 09-16-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.245.99.228	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
104.167.6.84	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
199.229.254.214	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.180.8.100	147.237.77.243	South Africa	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.235	Japan	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
104.245.99.228	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
104.245.99.228	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
101.178.206.92	147.237.8.50	Australia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.197.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
64.137.168.128	147.237.0.15	Canada	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
179.43.141.198	147.237.76.199	Switzerland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.77.233	Japan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.11.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-16-2016-10:04:06 to 09-16-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.125.22.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.69.36.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.205.224	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.117.75.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.4.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.43.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.131.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.181.230.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.168.205.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.46.38.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.41	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
31.168.0.253	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.166.114.235	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.98.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
2.53.25.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
31.168.0.253	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.108.33.192	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.253.130.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
85.64.215.33	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.159.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.229.197	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
37.46.38.238	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
64.246.165.160	United States	147.237.77.170	maarachot.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
46.19.85.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
80.179.22.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
101.178.206.92	Australia	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
80.178.98.149	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
2.53.46.10	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.253.130.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.29.84.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-16-2016-10:04:06 to 09-16-2016-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.53.50.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.116.30.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	6
46.19.86.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.185.70	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
77.124.23.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
109.65.20.120	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.180.185.70	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.180.185.70	Block	1
212.150.214.90	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
89.237.71.126	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
81.5.172.102	United Kingdom	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
176.13.236.140	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
213.57.158.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl75 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
91.241.146.147	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
31.168.205.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
180.76.15.18	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.180.185.70	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
216.244.66.231	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.117.75.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.102.49.193	Netherlands	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
77.124.43.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
185.89.217.233	Netherlands	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	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
79.182.37.112	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.102.9.5	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
104.128.144.131	Canada	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/redirect.php	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
79.177.171.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
207.46.13.42	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
80.178.98.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1

09-16-2016-10:04:06 to 09-16-2016-11:04:06