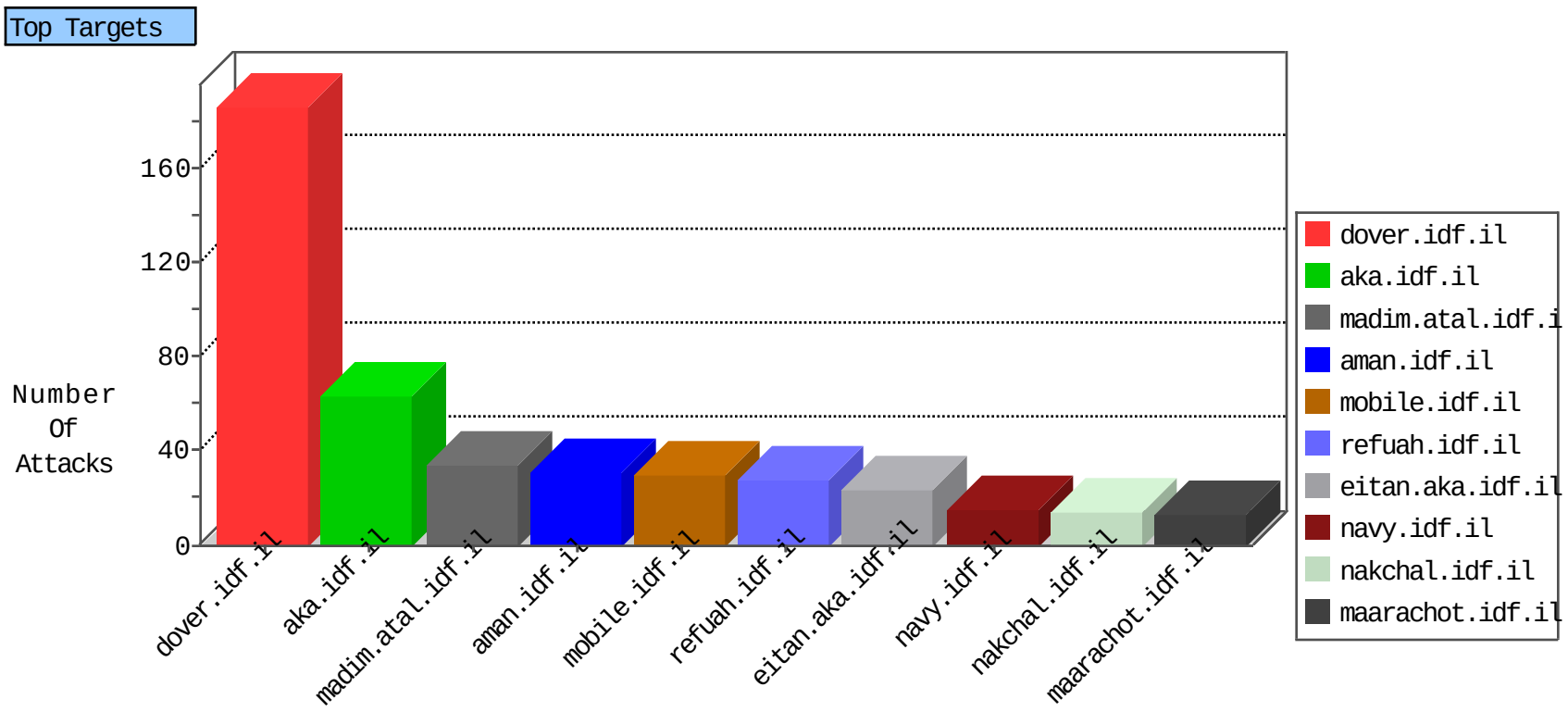
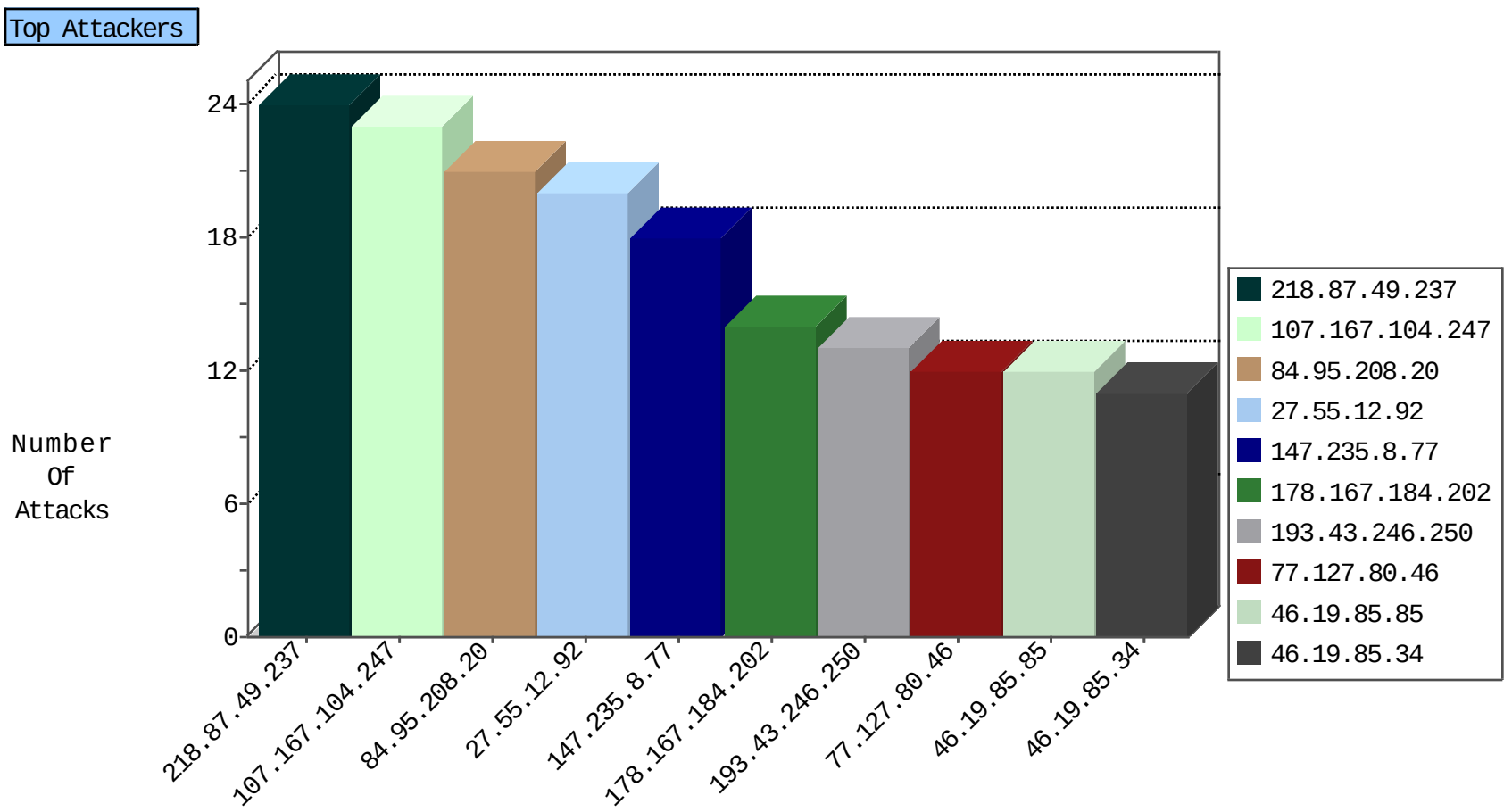
09-23-2016-11:04:02 to 09-23-2016-12:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-23-2016-11:04:02 to 09-23-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.167.184.202	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
5.28.140.183	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.26.149.172	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
123.151.149.222	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
121.127.7.55	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
121.127.7.48	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
123.151.149.222	China	147.237.0.19	madim.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
121.127.7.49	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
121.127.7.51	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.244.198.5	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
114.79.8.213	Indonesia	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-23-2016-11:04:02 to 09-23-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.56.155.81	China	147.237.77.170	maarachot.idf.il	C1000016: HTTP: administrator in URI	Permit	6
195.154.187.115	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.56.155.81	China	147.237.77.170	maarachot.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-23-2016-11:04:02 to 09-23-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
100.13.130.4	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
216.81.230.167	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.231.57	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 4096	1
210.212.207.80	147.237.8.14	India	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
188.161.81.184	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	1
91.201.236.50	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.173	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
113.240.250.154	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
211.149.231.57	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.235	Ukraine	sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
211.149.197.148	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 3072	1
210.212.207.80	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.238.45	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
71.15.85.176	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
121.136.74.10	147.237.77.205	Korea, Republic of	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.63.28.189	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
108.38.107.213	147.237.76.42	United States	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-23-2016-11:04:02 to 09-23-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.104.247	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
27.55.12.92	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
77.127.80.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.92.1.206		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
100.92.115.216		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
77.138.51.90	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.246.137.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.197.85	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.235.8.77	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.120.154.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.167.184.202	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
147.235.8.77	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.77	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.148.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.148.182	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
46.210.245.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.182.131.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.142	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.211.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.27.76	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.85	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.210.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.122	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
178.167.184.202	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
147.235.8.77	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.24.207.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.49.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
147.235.8.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.178.101.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.24.207.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.189.226	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.147.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.117.30.115	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.44.203	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.111.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.120.148.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.182	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.126.87.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.102.253.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.80.241	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.168.24.252	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-23-2016-11:04:02 to 09-23-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
218.87.49.237	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.87.49.237	Block	17
2.55.8.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
218.87.49.237	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
2.55.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
2.53.30.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.140.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.102.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.132.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.141.79	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 80.246.141.79	Block	3
109.253.208.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.149.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
2.53.153.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.125.12.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
212.25.85.54	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.85.54	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1779-21525-he/idfgdover.aspx	Block	1
31.154.81.71	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
84.108.244.43	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/div.item	Block	1
80.246.137.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
218.87.49.237	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
141.226.217.240	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	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
213.57.243.74	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.93.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
31.154.81.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
94.41.125.90	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/'	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
147.235.8.77	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
37.26.148.183	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
147.235.8.77	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
66.249.69.186	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
77.249.173.146	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.194.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
80.246.141.79	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-touch-icon-120x120-precomposed.png	Block	1
188.120.154.128	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.73.176	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/m/	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1

09-23-2016-11:04:02 to 09-23-2016-12:04:02