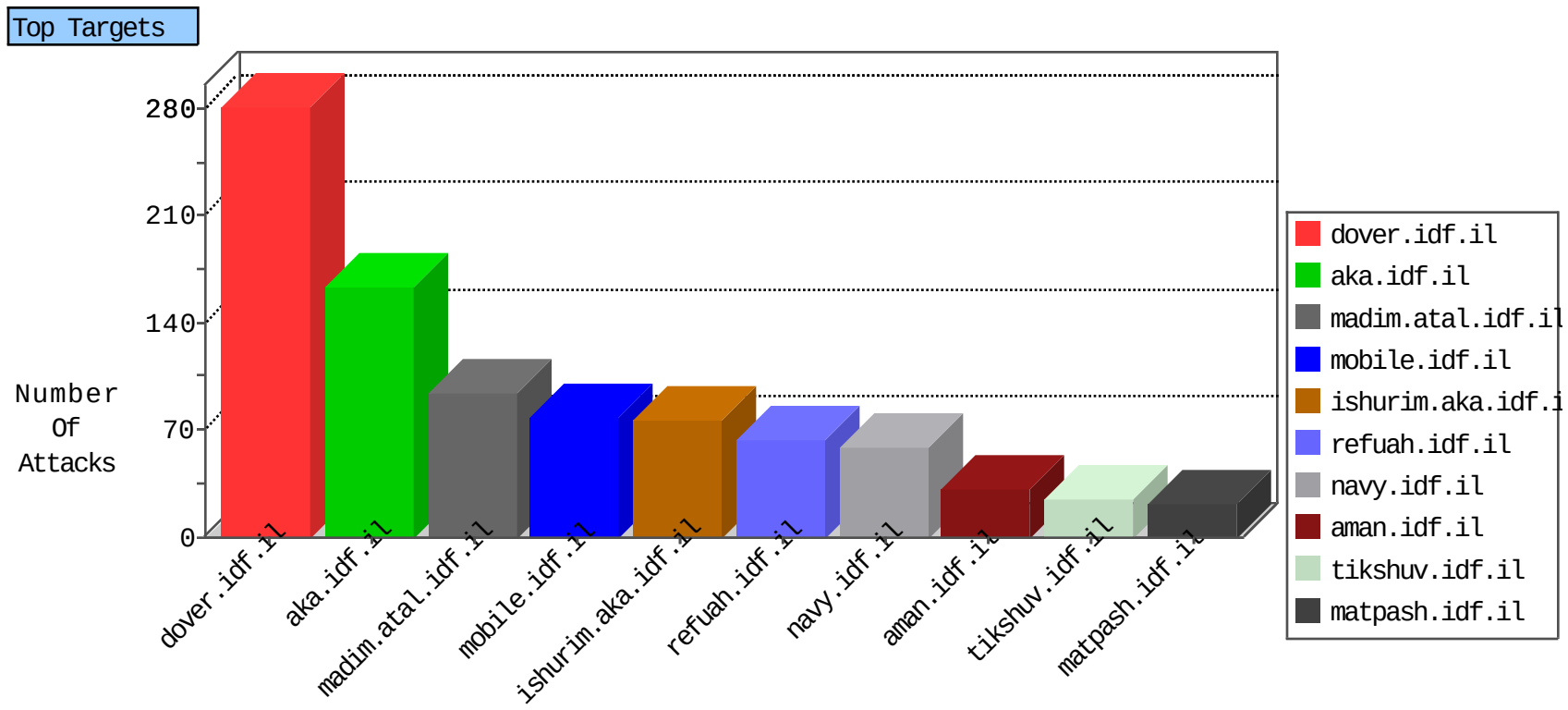
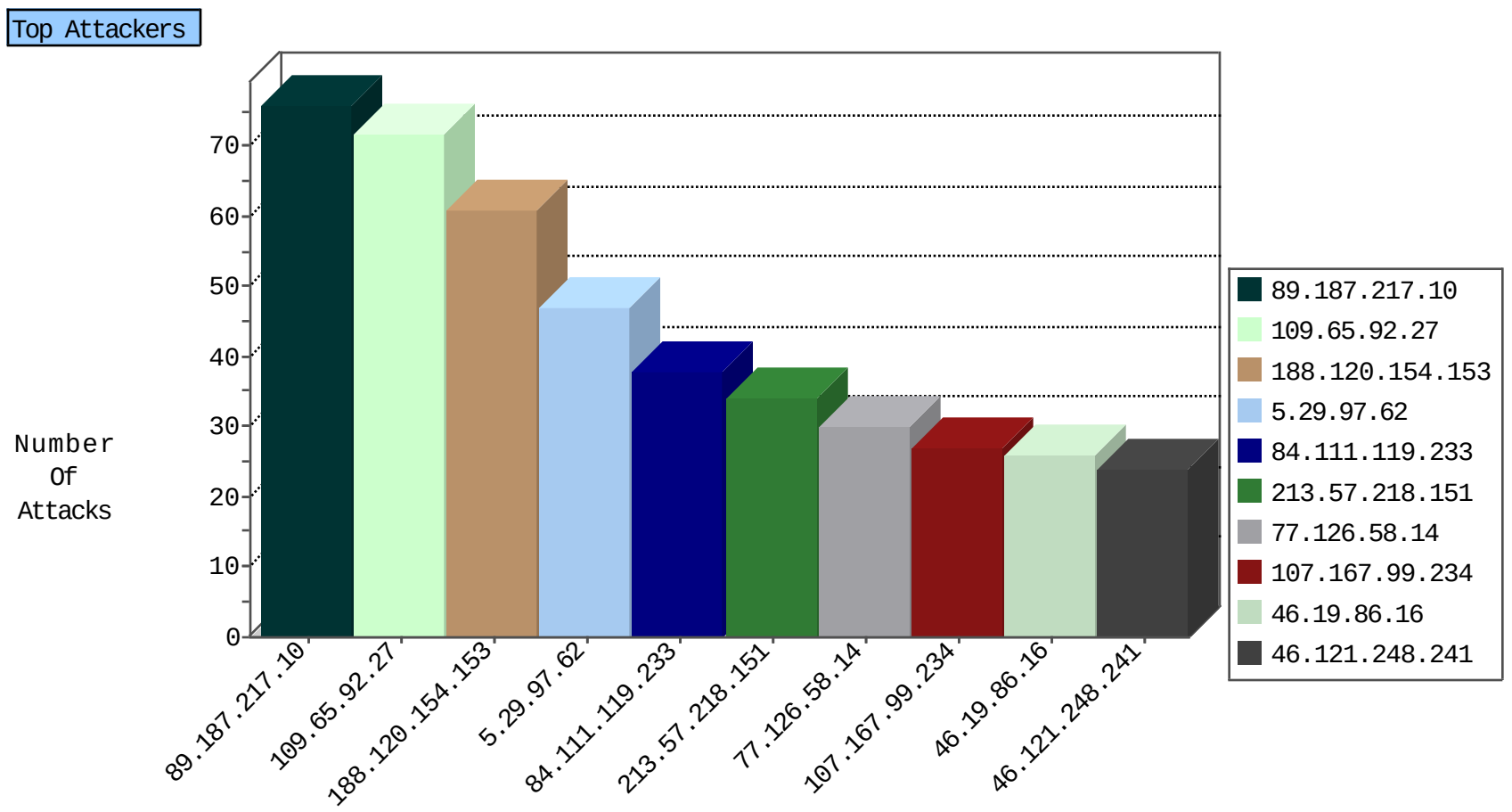
09-20-2016-19:04:09 to 09-20-2016-20:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-19:04:09 to 09-20-2016-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.218.151	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
109.253.214.7	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-20-2016-19:04:09 to 09-20-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	4
78.166.58.106	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
78.166.58.106	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
151.80.31.107	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-20-2016-19:04:09 to 09-20-2016-20:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.161.81.122	147.237.0.200	Taiwan	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
193.201.225.19	147.237.77.74	Ukraine	law.idf.il	ET SCAN Potential SSH Scan	1
41.160.222.18	147.237.0.200	South Africa	m4u.idf.il	ET SCAN Potential SSH Scan	1
95.156.251.10	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.19	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
14.216.221.202	147.237.76.201	China	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.91.29	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.19	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.225.19	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
217.174.61.176	147.237.8.24	Bulgaria	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.1.174	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
211.149.231.57	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
41.230.31.128	147.237.77.61	Tunisia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.19	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
41.203.87.2	147.237.76.86	Nigeria	navy.idf.il	ET SCAN NMAP -sS window 3072	1
118.103.126.194	147.237.0.15	Japan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.19	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
27.75.84.16	147.237.72.156	Vietnam	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.156.251.10	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.19	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.19	147.237.72.156	Ukraine	aman.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
164.52.227.101	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
68.180.229.223	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
216.218.206.80	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
151.11.201.3	147.237.77.19	Italy	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
41.230.31.128	147.237.77.61	Tunisia	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
211.149.222.5	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.83.162	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.19	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN Potential SSH Scan	1
41.203.87.2	147.237.76.86	Nigeria	navy.idf.il	ET SCAN NMAP -sS window 4096	1
118.103.126.194	147.237.76.201	Japan	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-19:04:09 to 09-20-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.187.217.10	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
188.120.154.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
109.65.92.27	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	32
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
107.167.99.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	27
84.111.119.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
185.26.180.72	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
109.65.92.27	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
41.140.18.189	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.121.248.241	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.121.248.241	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.65.92.27	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
82.205.11.43	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.92.27	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.65.92.27	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.58	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.46.39.179	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.121.26.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.143.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.218.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.123.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
213.57.218.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.135	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.172.231.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.246.136.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.108.123.180	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.127.21.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
77.138.53.201	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.3.147.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.157.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.32.179.167	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
217.246.252.53	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.28.154.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
77.127.21.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.133.242.3	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.11.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.5.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.137.28	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.3.147.179	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.76.149	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.102.254.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-20-2016-19:04:09 to 09-20-2016-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.97.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
84.111.119.233	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.111.119.233	Block	11
109.253.221.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.136.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.174.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.245.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.167.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.37.102	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	2
37.142.230.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	2
77.125.55.57	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
94.254.178.144	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.116.22.215	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.22.215	Block	2
37.26.149.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.176.49	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple NULL Character in Method from 195.154.14.134	Block	1
188.214.55.210	Romania	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
66.102.8.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-he/+navmenu.qc+	Block	1
84.229.63.39	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
213.57.104.146	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
68.180.231.35	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal HTTP Version À[[#20]]À	Block	1
109.253.143.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/piwik.php	Block	1
2.53.43.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.196.196	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
192.116.167.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.102.9.8	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
5.29.120.21	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
93.169.11.180	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
80.246.140.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed HTTP Header Line 1	Block	1
84.108.86.57	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
2.53.62.3	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in URL •¶@[[#3]]iÛ×j.[[•Ð#0[[]]#0[[]]#28.+./.]]0..,[[#19]].	Block	1
79.177.227.23	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
66.102.9.152	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
5.29.159.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdateQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
84.94.32.197	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
77.125.88.234	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL •¶@[[#3]]iÛ×j.[[•Ð#0[[]]#0[[]]#28.+./.]]0.[[.,#19.]]	Block	1
157.55.39.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/changelog.txt	Block	1
79.178.14.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oreg	Block	1
195.154.14.134	France	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
66.249.64.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.64.24.76	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

09-20-2016-19:04:09 to 09-20-2016-20:04:09