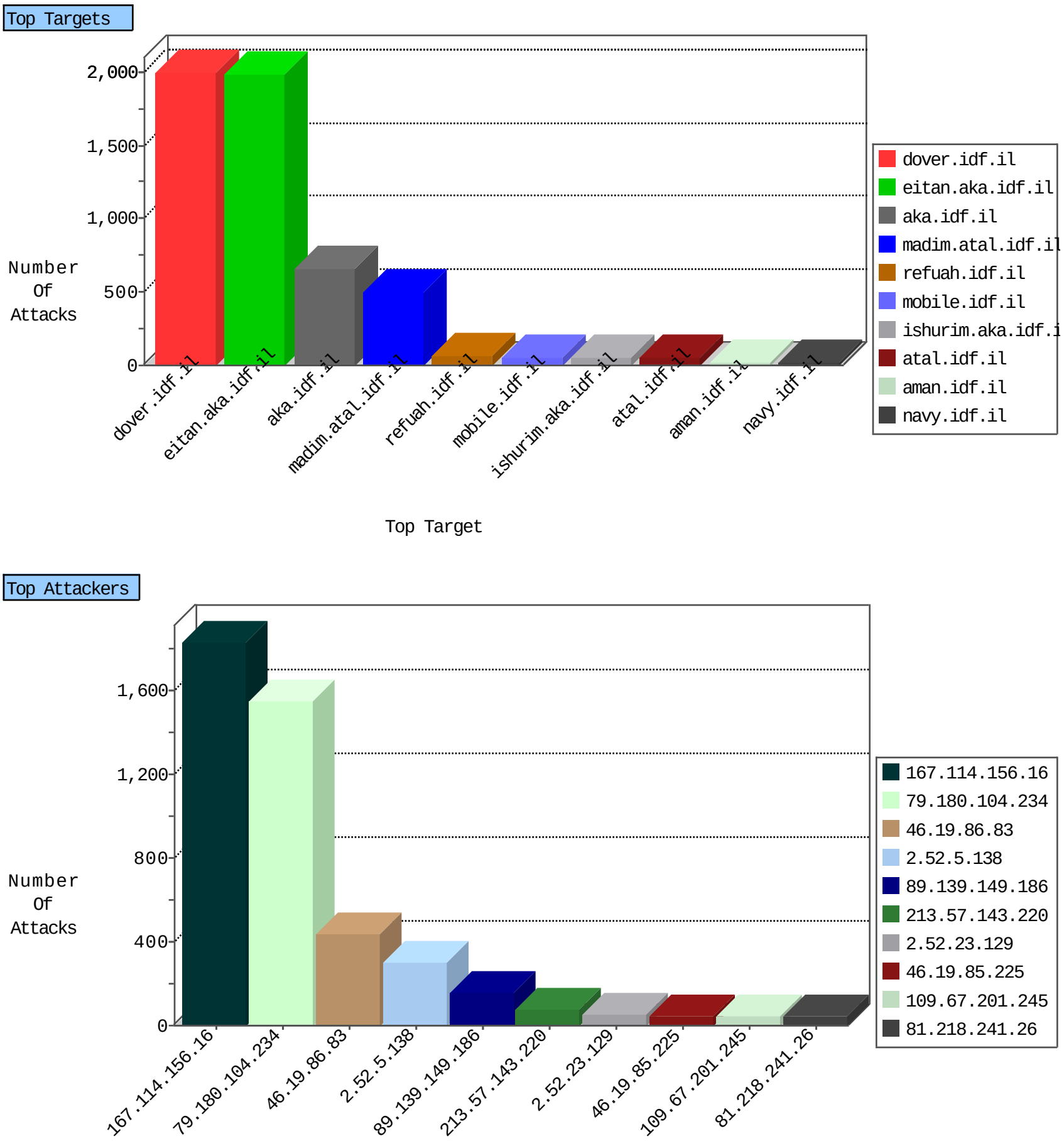
12-20-2015-11:04:09 to 12-20-2015-12:04:09

IDF Under Attack Daily Report



12-20-2015-11:04:09 to 12-20-2015-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3153
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	421
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
62.90.9.250	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	64
176.13.11.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.180.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
213.57.119.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-20-2015-11:04:09 to 12-20-2015-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.66	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.200	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.120.156.17	Israel	147.237.72.166	aka.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1

12-20-2015-11:04:09 to 12-20-2015-12:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
178.187.73.209	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
193.104.41.54	147.237.76.201	Moldova, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.44	Moldova, Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
178.187.73.209	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
178.187.73.209	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
176.13.0.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.194.59.77	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.228.33.167	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
211.95.59.227	147.237.77.170	China	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.60.89	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.72.217	Sweden	e.idf.il	ET SCAN NMAP -sS window 1024	1
62.0.67.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.199	Moldova, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.54	147.237.76.31	Moldova, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
178.187.73.209	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
178.187.73.209	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
176.13.10.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
166.63.122.229	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
220.194.59.77	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
109.64.54.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.160.240.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.199.188.6	147.237.77.216	Ukraine	dover.idf.il	portscan: TCP Distributed Portscan	1

12-20-2015-11:04:09 to 12-20-2015-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.104.234	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1323
46.19.86.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	405
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	125
213.57.143.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.205.124	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	23
31.168.152.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
31.168.71.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.47.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.178.146.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.201.245	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
81.218.190.42	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
109.186.164.109	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
94.159.170.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
84.229.179.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
94.159.170.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
176.13.1.101	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.138.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.9.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.218.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.63.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.192.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.23.141	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
195.60.232.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.32.179.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.126.237.217	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.148.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.187.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.229.179.211	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.235.98.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.219.130.136	Israel	147.237.0.35	akaws.idf.il	drop		drop	5
85.130.218.128	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.124	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.1.101	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.131.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.246	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.130.216.49	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
64.246.165.10	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	4

12-20-2015-11:04:09 to 12-20-2015-12:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.104.234	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	227
2.52.5.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
2.52.5.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	142
2.52.23.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
109.67.201.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.86.83	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
2.52.5.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	14
80.246.136.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.52.138.175	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	7
176.13.17.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.179.68.209	Block	5
50.62.176.36	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.62.176.36	Block	5
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 89.139.149.186	Block	3
213.57.164.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/default.asp	Block	3
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	3
82.166.164.112	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.166.164.112	Block	3
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 89.139.149.186	Block	3
212.143.233.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
95.108.132.172	Russian Federation	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 89.139.149.186	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 89.139.149.186	Block	3
109.253.144.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.164.112	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	3
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.159.253	Block	3
176.13.18.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 89.139.149.186	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 89.139.149.186	Block	3
176.13.2.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 89.139.149.186	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 89.139.149.186	Block	3
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 89.139.149.186	Block	3
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	2
194.90.225.101	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	2
5.22.131.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
69.171.231.226	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
89.139.149.186	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 89.139.149.186	Block	2
87.68.71.148	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	2
212.68.132.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
109.253.216.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
120.61.41.109	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
37.26.147.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.11.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2

12-20-2015-11:04:09 to 12-20-2015-12:04:09