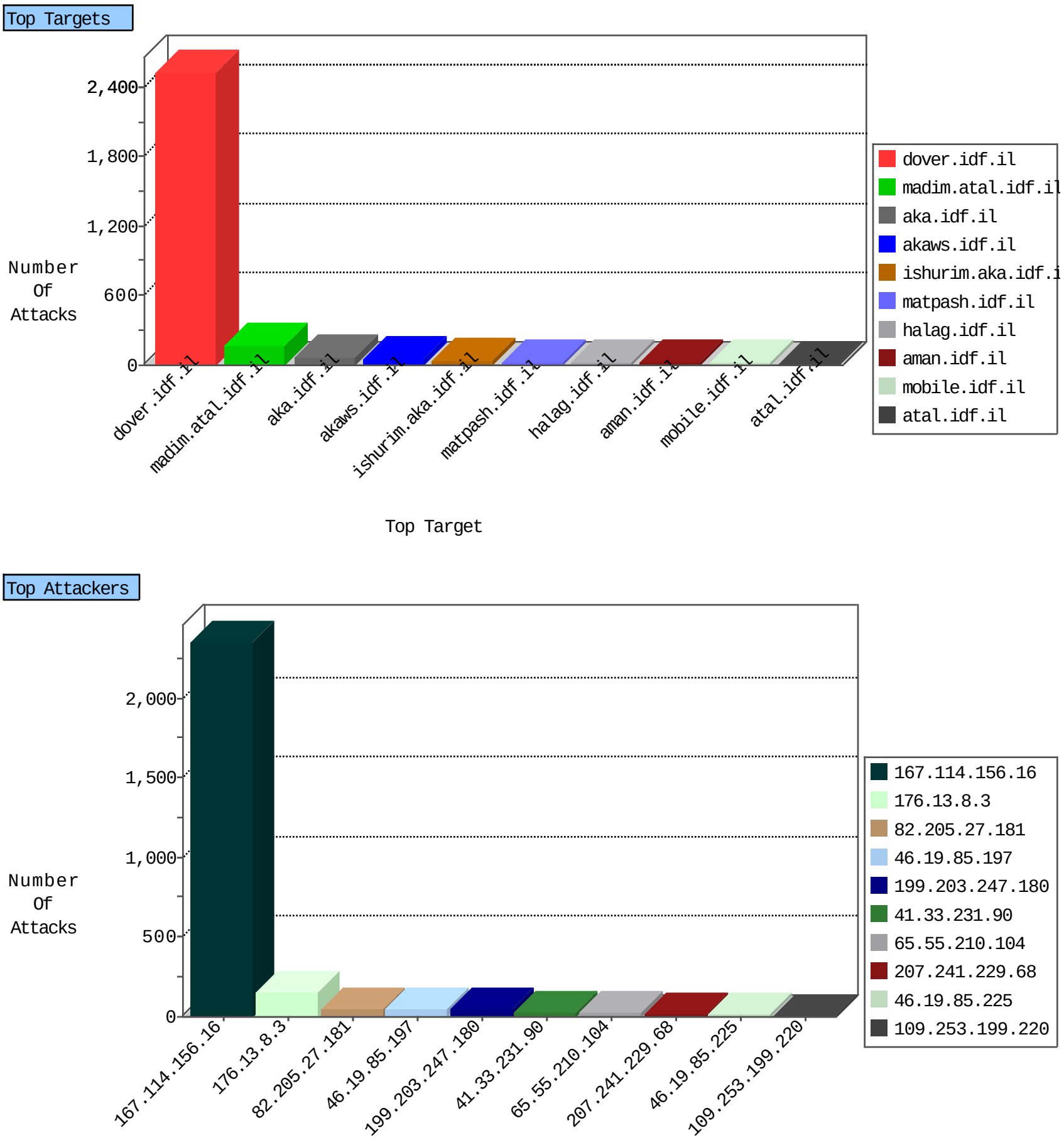
12-19-2015-00:04:09 to 12-19-2015-01:04:09

IDF Under Attack Daily Report



12-19-2015-00:04:09 to 12-19-2015-01:04:09

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	3526
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	208
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-19-2015-00:04:09 to 12-19-2015-01:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-19-2015-00:04:09 to 12-19-2015-01:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.180.26.24	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.253.199.220	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
84.245.15.57	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.191.56.188	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
199.191.56.188	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
46.219.254.51	147.237.0.15	Ukraine	kosher-kravi.idf.il	SERVER-WEBAPP admin.php access	1
146.185.250.2	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
84.245.15.57	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.205.27.181	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.191.56.188	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
24.121.225.29	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1

12-19-2015-00:04:09 to 12-19-2015-01:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.203.247.180	Israel	147.237.0.35	akaws.idf.il	drop		drop	44
46.19.85.197	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
65.55.210.104	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
82.205.27.181	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	19
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
46.19.85.197	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.247.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
46.19.85.225	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
130.207.203.56	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
185.32.179.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.205.27.181	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
149.78.71.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.225	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.253.199.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.199.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
184.73.194.60	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.180.196.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.142.68.98	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.127.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.179.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.4.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.212.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.65.34.177	Moldova, Republic of	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
204.79.180.87	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
162.209.124.35	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.7	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
94.159.178.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
84.109.50.129	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.177.155.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.131.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
157.55.39.194	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.59.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.131.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
85.65.199.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
46.19.85.209	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

12-19-2015-00:04:09 to 12-19-2015-01:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.8.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.8.3	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.8.3	Block	41
167.114.156.198	Canada	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	8
46.19.85.195	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	7
2.52.61.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
204.13.200.200	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 204.13.200.200	Block	3
79.183.185.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.49.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.219.254.51	Ukraine	147.237.0.15	kosher-kravi.idf.i	PHP Attempt	Block	2
79.178.4.186	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.219.254.51	Ukraine	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 46.219.254.51	Block	2
77.126.191.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
84.108.59.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 82.205.27.181	Block	1
199.115.117.117	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/_asterisk	Block	1
2.54.6.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL [[#0]]Â²7ÂµÆ'â€Ž×¥[[#0]]Â·h×˜Â«â„¢Ã œÂ¾>×™4vÂ¸Â»×±=qÂ²Â³×'[[#7]]ÂŒÃ›[â€ n[[#22]]%[[#28]]n[[#18]]-ÂŽtÂ¬]Â»fÂ¿$Â«Ã¿bÂ«n3×¥â€¢×–Â¸	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.133.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ the idf official website	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	NULL Character in Header Name at [[#11]]	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 82.205.27.181	Block	1
46.19.85.195	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.195	Block	1
178.62.82.172	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
109.67.172.56	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
84.109.81.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Malformed URL from 82.205.27.181	Block	1
46.219.254.51	Ukraine	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/wp-login.php	Block	1
37.26.147.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal URL Path Encoding [[#0]]Â²7ÂµÆ'â€Ž×¥[[#0]]Â·h×˜Â«â„¢Ã œÂ¾>×™4vÂ¸Â»×±=qÂ²Â³×'[[#7]]ÂŒÃ›[â€ n[[#22]]%[[#28]]n[[#18]]-ÂŽtÂ¬]Â»fÂ¿$Â«Ã¿bÂ«n3×¥â€¢×–Â¸	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	NULL Character in URL [[#0]]Â²7ÂµÆ'â€Ž×¥[[#0]]Â·h×˜Â«â„¢Ã œÂ¾>×™4vÂ¸Â»×±=qÂ²Â³×'[[#7]]ÂŒÃ›[â€ n[[#22]]%[[#28]]n[[#18]]-ÂŽtÂ¬]Â»fÂ¿$Â«Ã¿bÂ«n3×¥â€¢×–Â¸	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 82.205.27.181	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1414-17440-he/kkkkkkk=5b618702kkkkkkk_5b618702	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Ã¿ÂƒÂ¢Â¹Â›z[[#16]]cG	Block	1
149.88.109.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.199.179	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9757-he/refuah.aspx	Block	1
62.90.126.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 82.205.27.181	Block	1
40.77.167.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.8.3	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
82.205.27.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 13	Block	1

12-19-2015-00:04:09 to 12-19-2015-01:04:09