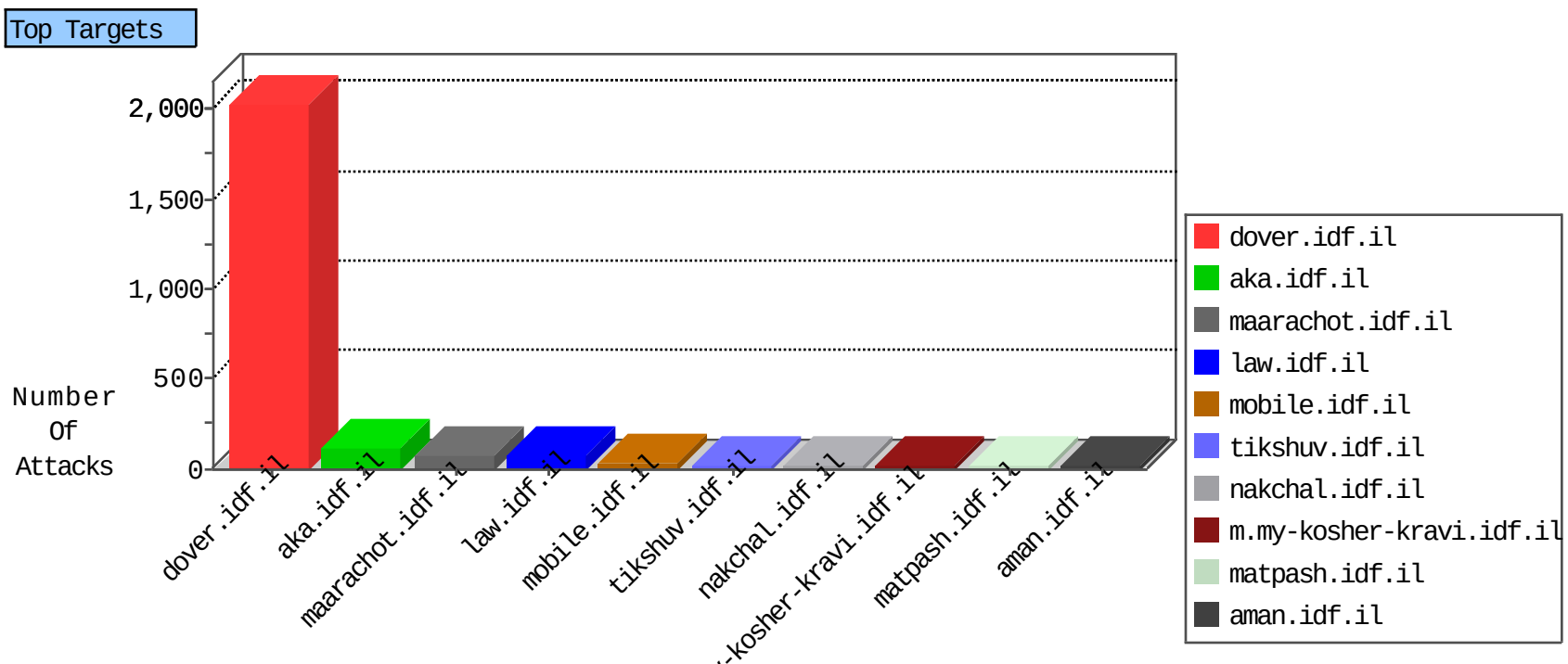
01-01-2016-23:04:01 to 01-02-2016-00:04:01

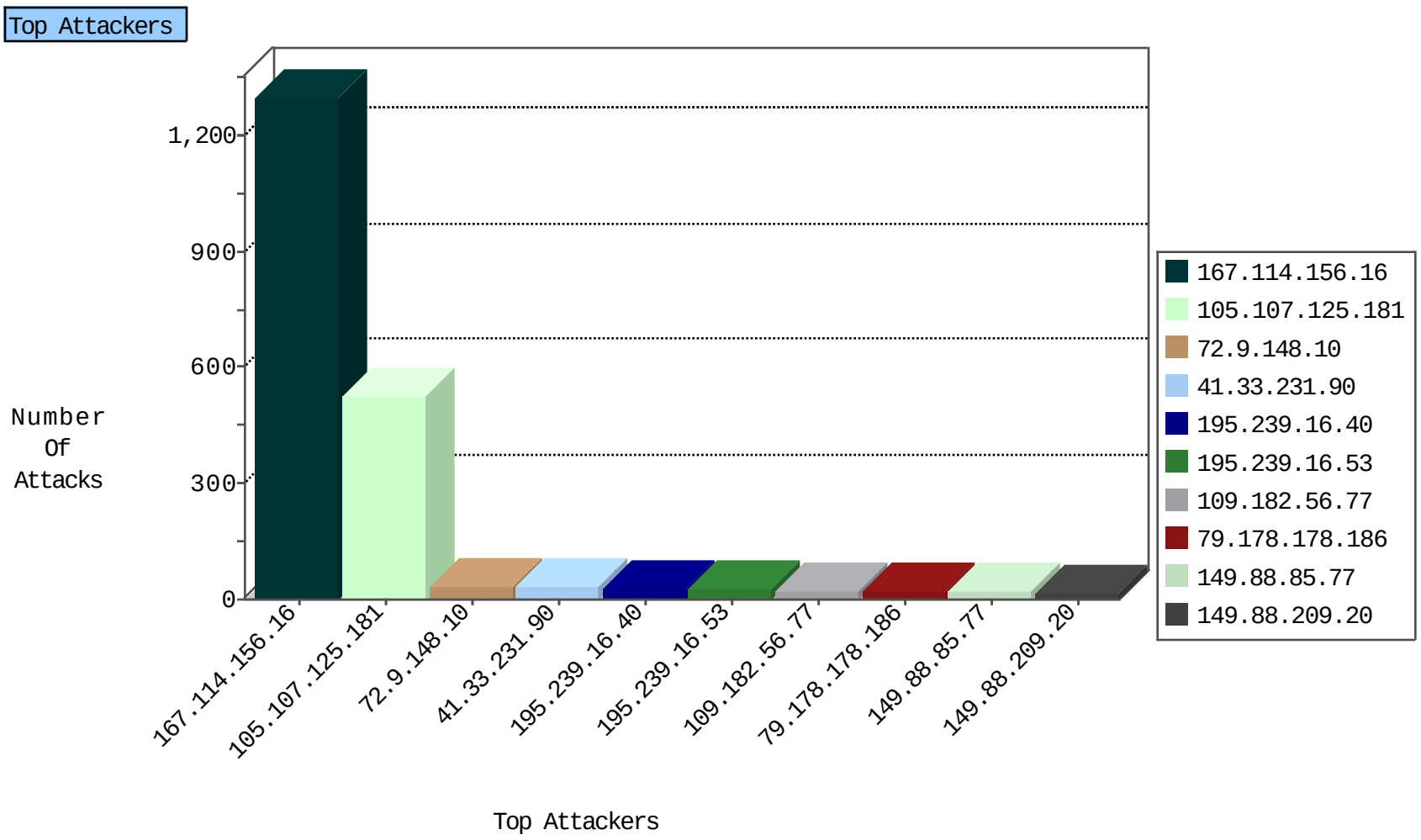
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-01-2016-23:04:01 to 01-02-2016-00:04:01

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	3152
110.9.184.159	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
110.9.184.159	Korea, Republic of	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-01-2016-23:04:01 to 01-02-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	26
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	2
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	C023: HTTP: administrator in URI	Permit	2

01-01-2016-23:04:01 to 01-02-2016-00:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
105.107.125.181	147.237.77.216	Algeria	dover.idf.il	Admin login page scan - Havij	21
105.107.125.181	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP admin.php access	6
105.107.125.181	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP adminlogin access	5
105.107.125.181	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP login.htm access	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
168.62.238.153	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.249.11	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
96.242.89.123	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
52.48.37.122	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.224	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
121.201.61.49	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
115.182.249.11	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
52.48.37.122	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
188.152.249.142	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
52.48.37.122	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
172.98.200.238	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 4096	1

01-01-2016-23:04:01 to 01-02-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
109.182.56.77	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.178.178.186	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	20
149.88.209.20	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.117.224.79	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.86.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.121.10	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
149.50.77.38	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
84.111.155.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.143	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.178.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
89.139.242.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
217.132.97.241	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
149.88.85.77	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.170.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.170.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.179.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.103.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.151.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.183.179.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.95	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
128.127.107.126	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.88.46.204	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.60.150	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.3.147.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
84.109.210.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.179.225.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.176.73.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.108.158.167	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.216.187	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.159.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.205.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.167.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.9	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.229.29.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.135.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-01-2016-23:04:01 to 01-02-2016-00:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.107.125.181	Block	281
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 105.107.125.181	Block	90
105.107.125.181	Algeria	147.237.77.216	dover.idf.il	PHP Attempt	Block	80
149.88.85.77	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.85.77	Block	15
79.178.28.206	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	12
89.138.68.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
176.13.1.224	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
37.26.146.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
85.250.23.119	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step2.aspx	Block	1
46.121.62.31	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.121	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
2.52.10.90	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
173.252.90.229	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Â©Â¥Ã” [[#3]]k[[#8]]Â¤*Â¬[[#24]]Ã¬Ã‰Ã´[[#12]]•A[[#21]]Â»Ã¦•ÃŒ DÃªÂ©[[#14]]bÂ¤Â?Â”feÃ²ÂƒCÃ‡[[#2]]Ã©Ã?3Ã¨Ã–Z3Ã”R[[#7]]aÂ§Â€ Ã?[[#17]]Â¦Ã†Â©Â£AfÃ²W•raÃƒ[[#19]]Â„Â¯Â©[[#3]]s[[#11]]ÂŠ^Ã¼ÃŸ d;[[#3]]Ã¬[[#29]][S[#5]]FÃ™ .ÂŠ(Â?Ã€Ã½Ã§ÃºÂ[[#6]]5&4*..Â–zÂ˜W •Â„Ã¼Â¯Â•Ã¡A%Â’[[#12]]Â³oÃ¸ [[#29]]Â•Âƒ[[#22]]Ã…eC[[#23]]<Ã‡ Ã?\Ã²[[#21]][[#3]]#Ã¤Â?1c>Ã¯Ã·Â‹ÂŒÂ·ÃˆjÃ¼GÂªÃ‚7ÃŒÃ––	Block	1
109.65.181.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.182.70.173	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
213.8.204.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.146.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
173.252.115.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 1	Block	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	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
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
46.166.186.226	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.46.13.144	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
2.52.14.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.240	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
109.201.154.235	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.182.197.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.142.230.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
173.252.88.182	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.177.16	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
79.177.59.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.99.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
51.39.46.11	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
2.52.49.157	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
173.252.90.249	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.177.246	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method Â®[[#8]]Â¡[[#18]]ÃŽ 5Ã¢rr[[#31]]Ã½Ã¶Ã’D9Â¥[[#23]]Âž@Â-Â¨[[#29]]OÂ¿[[#17]]Ã„ {[[#3]]HA`Ã‘(Â·_Âƒ[[#3]]Ã¸ Â™Â› [[#7]]Ã¿[[#4]][[#8]]"GR3Ã±8Ã¢k0Ã¦[[#23]]Â¥WÃ»,Ã–Â¢ÃœAÂ–Ã°~Âž Â·Â«n&5ÃžÃ˜Â²Ã¤Â«[[#14]][[#26]][[#29]]Â¶ IAAÂ±[[#30]][[#24]]Â¨ÃŽ%[[#4]]Ã¬Ã¼>cÃƒÂ‚Â‹XÂ²[[#28]]Ã£A,Ã™ C9Âš}Â‘pBÃ–Ã¯&ÃŸV	Block	1
109.253.135.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.183.176.19	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
84.109.210.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

01-01-2016-23:04:01 to 01-02-2016-00:04:01

01-01-2016-23:04:01 to 01-02-2016-00:04:01