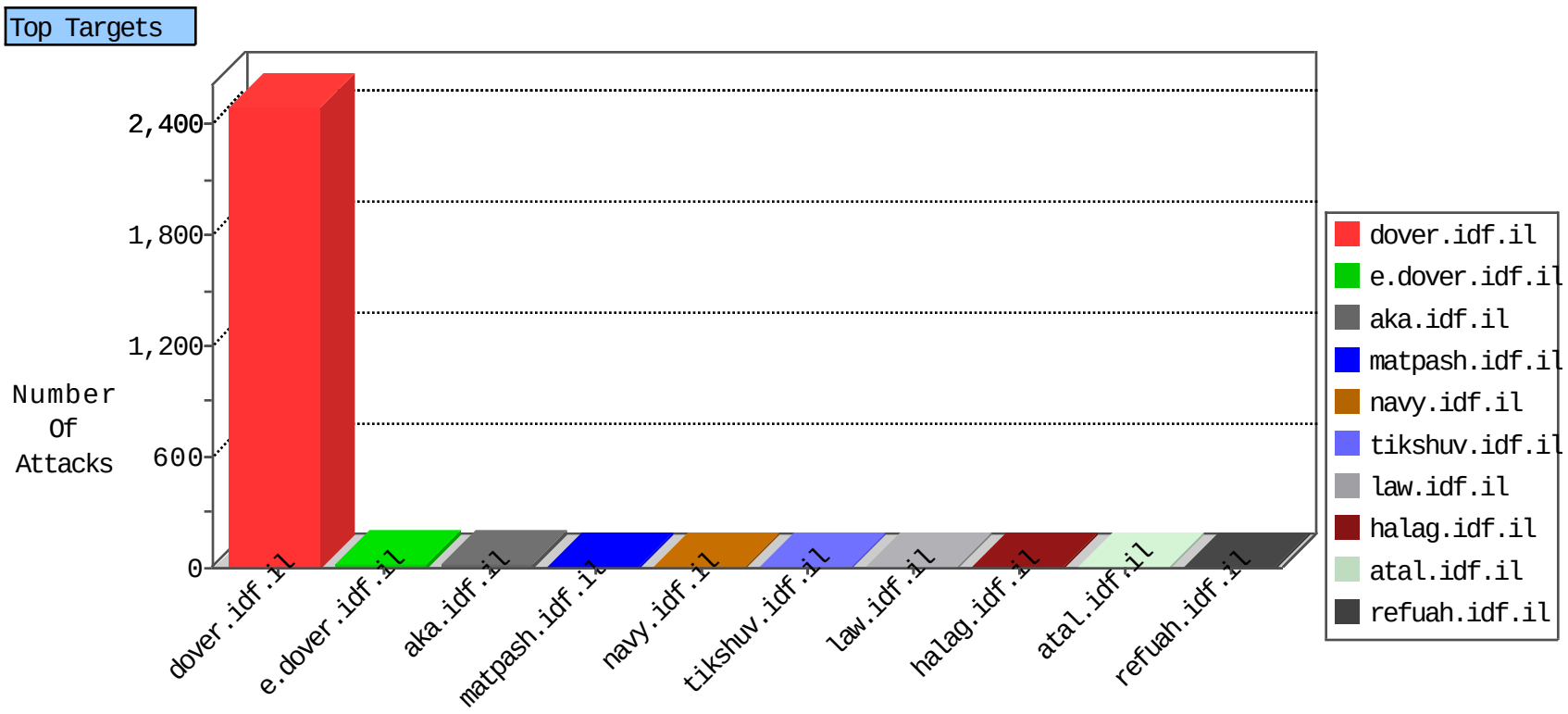
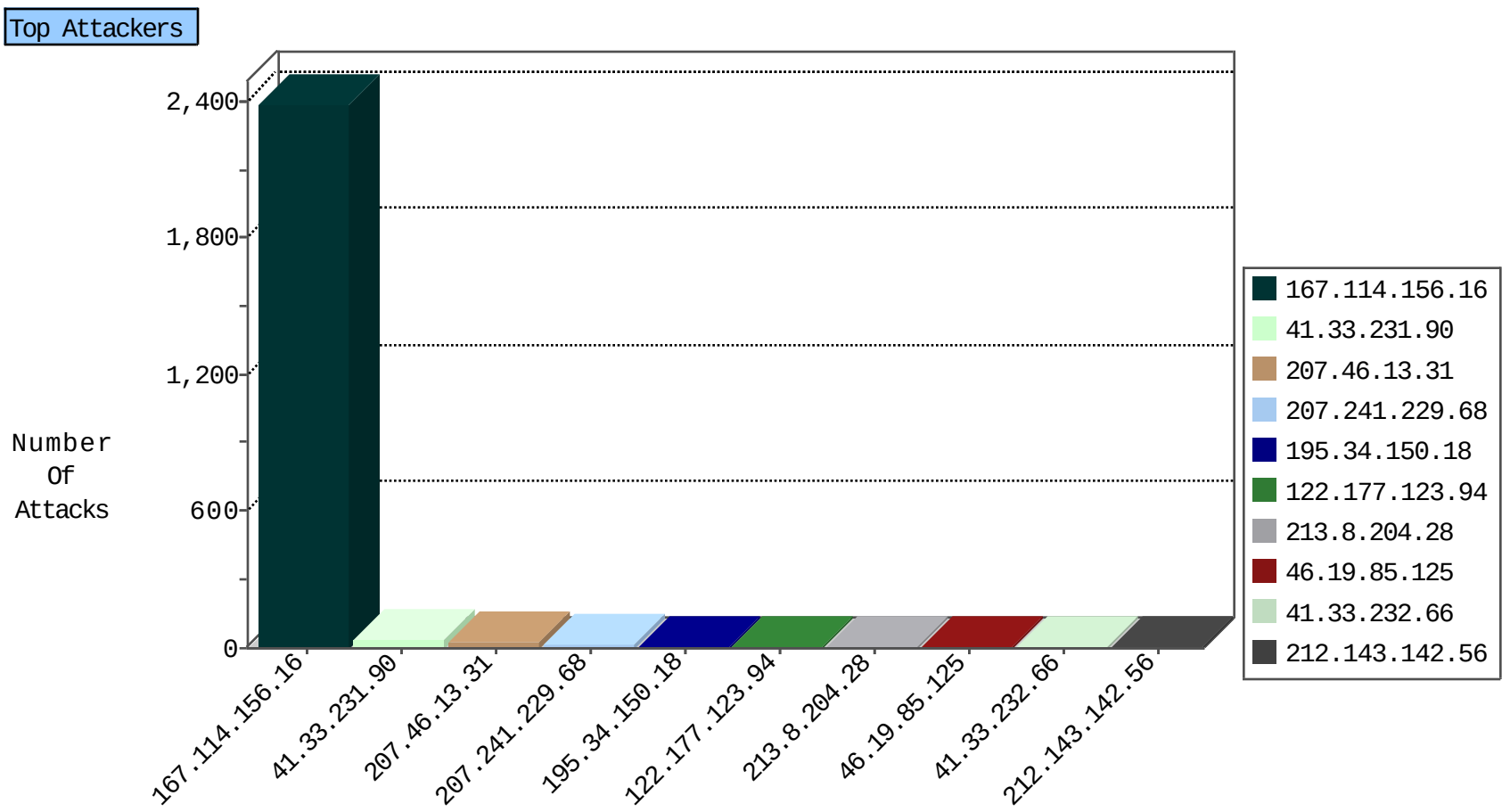
12-19-2015-07:04:00 to 12-19-2015-08:04:00

IDF Under Attack Daily Report





12-19-2015-07:04:00 to 12-19-2015-08:04:00

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	3513
172.98.67.123		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

12-19-2015-07:04:00 to 12-19-2015-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-19-2015-07:04:00 to 12-19-2015-08:04:00

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
95.45.254.123	147.237.77.216	Ireland	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
199.16.31.170	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
190.249.184.162	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
183.87.140.52	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.185.250.2	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
199.16.31.170	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
190.249.184.162	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.116	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
104.43.236.38	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
199.16.31.170	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1

12-19-2015-07:04:00 to 12-19-2015-08:04:00

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	34
207.46.13.31	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	21
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
207.46.13.143	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.206	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.125	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
176.13.1.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.3.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.105	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.220.156.105	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
38.229.1.15	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
92.96.74.124	United Arab Emirates	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.27	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
184.105.247.231	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.4.109.148	Germany	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
184.105.139.108	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
142.4.105.172	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.48	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.223	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.1.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
74.82.47.27	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.231	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.4.109.148	Germany	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.199	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.78.11.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
85.64.39.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.223	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
74.82.47.27	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.125	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.251.209.165	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.11.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.111.209	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.223	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.90	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
213.8.204.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.105	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]]$<[[#16]]ÂŒÃ„mSÃ“Â‹[[#1]]Ã¶m[[#18]]OÂ¸BYÃ¡[[#24]]y[[#12]]Â¯!rc[[#18]]Ã’Ã‹[[#12]]Ã?[[#1]]g:[[#5]]Ã±Â–Âž[[#4]]J8I3JÂ§q/Â¨JÃ£Ã–	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name kÂ¿ÃŠÃ”Ã™AÂ?Ã?Â†Ã„•Â,Â…[[#20]][[#18]]qÃµ>'ÃŒ[[#16]]Ãƒ[[#15]]-Ã½Ã¾Ãª[[#22]]Â²<6fÃ¾tÃ?QjÃ‹ÃŽÃ„Â¥Ãžb/,Ã,Ã©Â?"Ã»[[#28]][[#6]]T[[#19]]`mTrtÂ›Ã¯-Ã,	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1
40.77.167.105	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.105	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]]$<[[#16]]ÂŒÃ„mSÃ“Â‹[[#1]]Ã¶m[[#18]]OÂ¸BYÃ¡[[#24]]y[[#12]]Â¯!rc[[#18]]Ã’Ã‹[[#12]]Ã?[[#1]]g:[[#5]]Ã±Â–Âž[[#4]]J8I3JÂ§q/Â¨JÃ£Ã– in URL	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
37.26.149.143	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.26.149.143 (sigalgs DoS Attack)	None	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
46.19.85.125	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
131.253.25.199	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/i/jot	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.223	Block	1
207.46.13.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/	Block	1
40.77.167.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1137-he/dover	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]]$<[[#16]]ÂŒÃ„mSÃ“Â‹[[#1]]Ã¶m[[#18]]OÂ¸BYÃ¡[[#24]]y[[#12]]Â¯!rc[[#18]]Ã’Ã‹[[#12]]Ã?[[#1]]g:[[#5]]Ã±Â–Âž[[#4]]J8I3JÂ§q/Â¨JÃ£Ã–	Block	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	1
213.8.204.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.28	Block	1
40.77.167.105	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.105	Block	1
122.177.123.94	India	147.237.76.86	navy.idf.il	Malformed URL	Block	1
95.45.254.123	Ireland	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

12-19-2015-07:04:00 to 12-19-2015-08:04:00