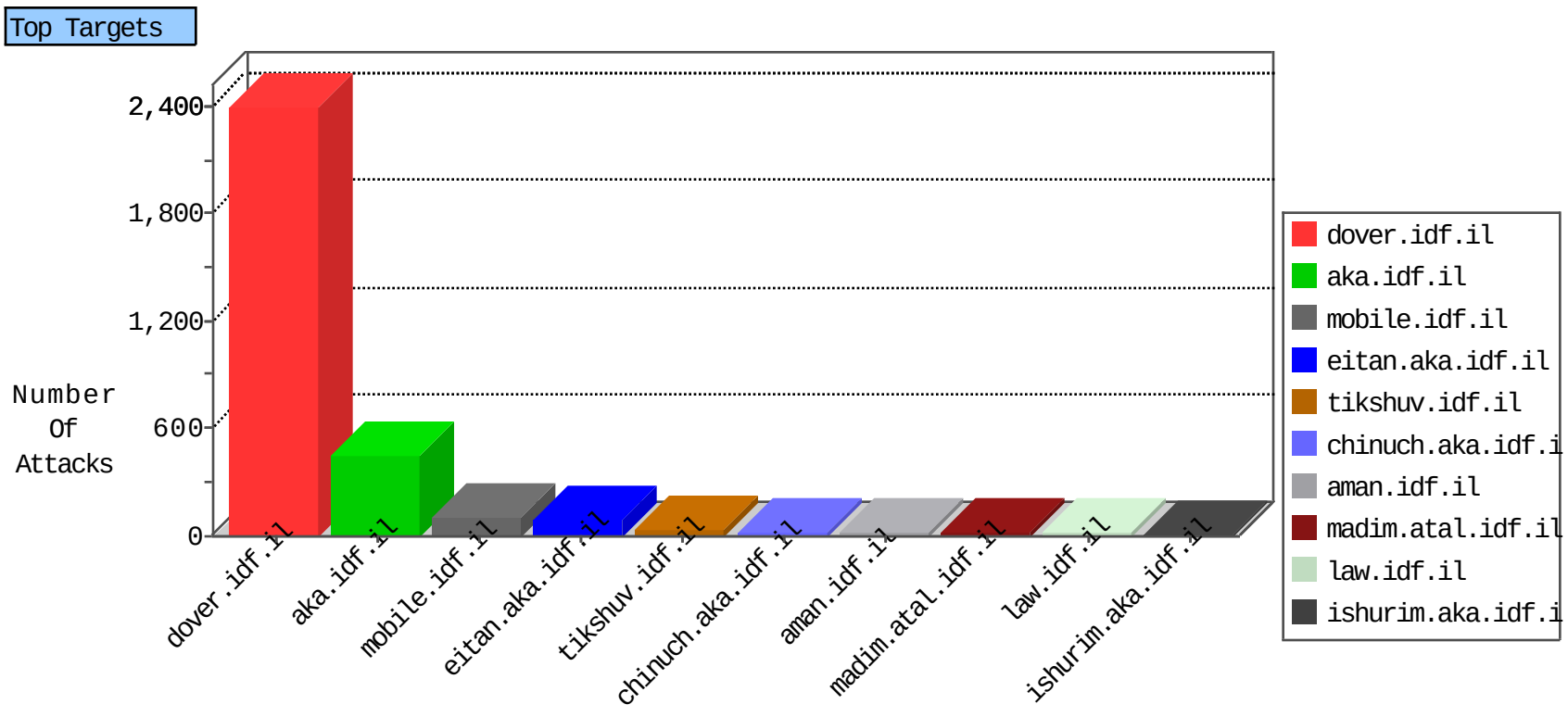
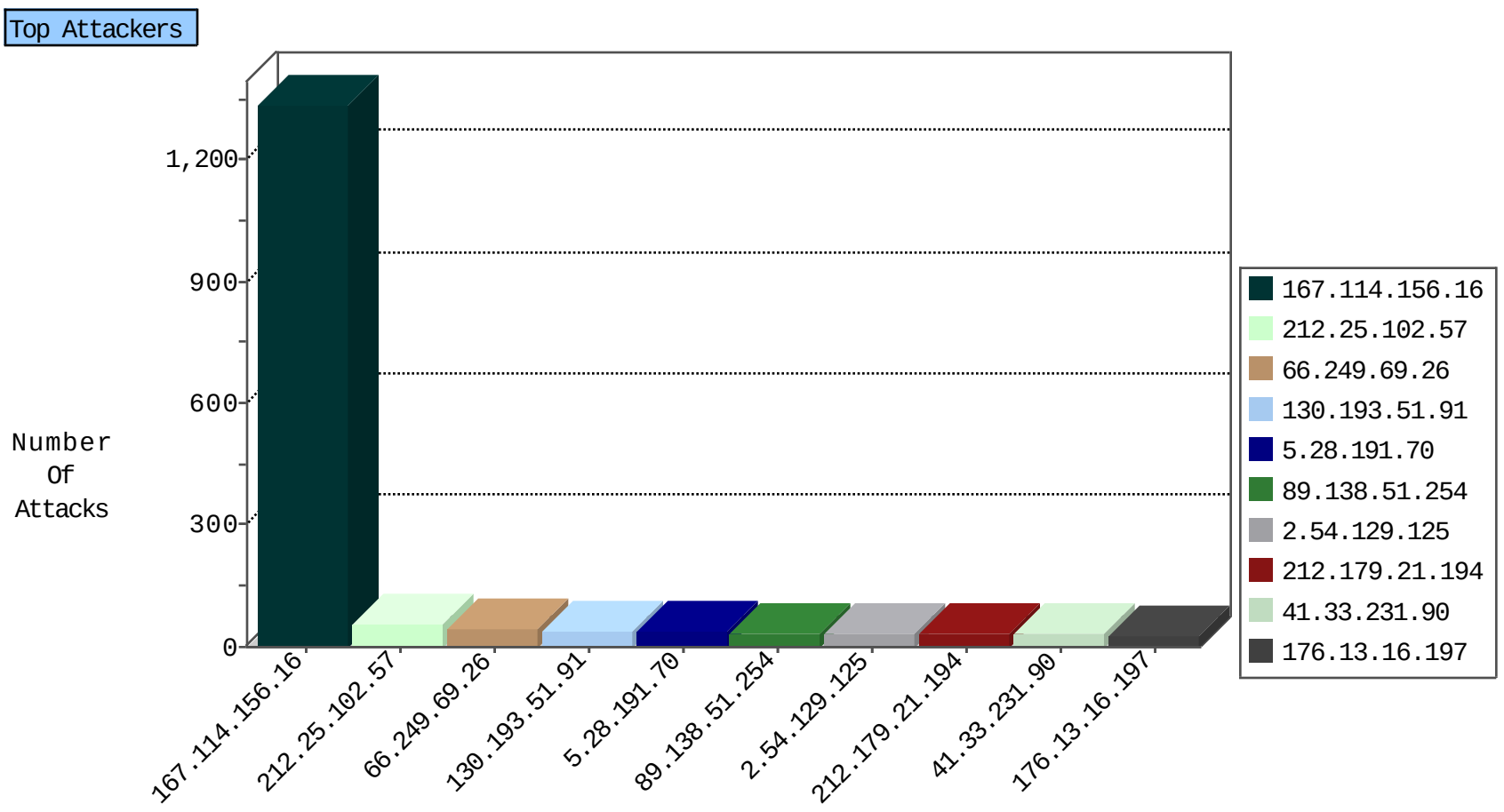
12-31-2015-14:04:04 to 12-31-2015-15:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-31-2015-14:04:04 to 12-31-2015-15:04:04

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	3109
109.65.190.174	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
106.75.199.192	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
107.150.98.128	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

12-31-2015-14:04:04 to 12-31-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-31-2015-14:04:04 to 12-31-2015-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.138.224.206	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	5
5.102.255.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
163.247.46.239	147.237.77.216	Chile	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.143.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.242.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.177	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.160.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.88.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
134.191.232.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.134.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.93.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.177	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.26	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.147.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-31-2015-14:04:04 to 12-31-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
5.28.191.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
89.138.51.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
213.8.63.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
109.253.128.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.50.94.177	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
87.68.255.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.142.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
176.13.3.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.176.80.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.208.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.214.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.127.165.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
79.181.32.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.202.194	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.52.149.219	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.186	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.89.217.227		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.142.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
2.52.149.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.219.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.0	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.94.48.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.142.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
2.54.142.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
113.190.238.6	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.149.219	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.84.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.25.102.57	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.107.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.142.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.98.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.196.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.167.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
2.54.129.125	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	35
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
176.13.16.197	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
62.0.6.226	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
213.151.38.154	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
46.116.177.17	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
176.13.2.11	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
109.253.207.1	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
77.125.87.137	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.247.74.58	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
109.253.159.111	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
91.208.139.250	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
84.228.8.160	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.228.8.160	Block	14
176.13.17.244	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.4.117	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.52.35.81	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.171	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.2.35	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.253.156.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.81	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.196	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.253.212.46	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
149.78.86.247	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
5.102.213.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
2.54.52.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
212.25.102.57	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	9
213.57.108.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.67.115.125	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
212.29.225.78	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
2.54.133.43	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
157.55.39.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	8
37.46.39.10	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
176.13.3.154	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
89.138.51.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
2.54.54.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
109.65.163.91	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
212.150.87.181	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

12-31-2015-14:04:04 to 12-31-2015-15:04:04