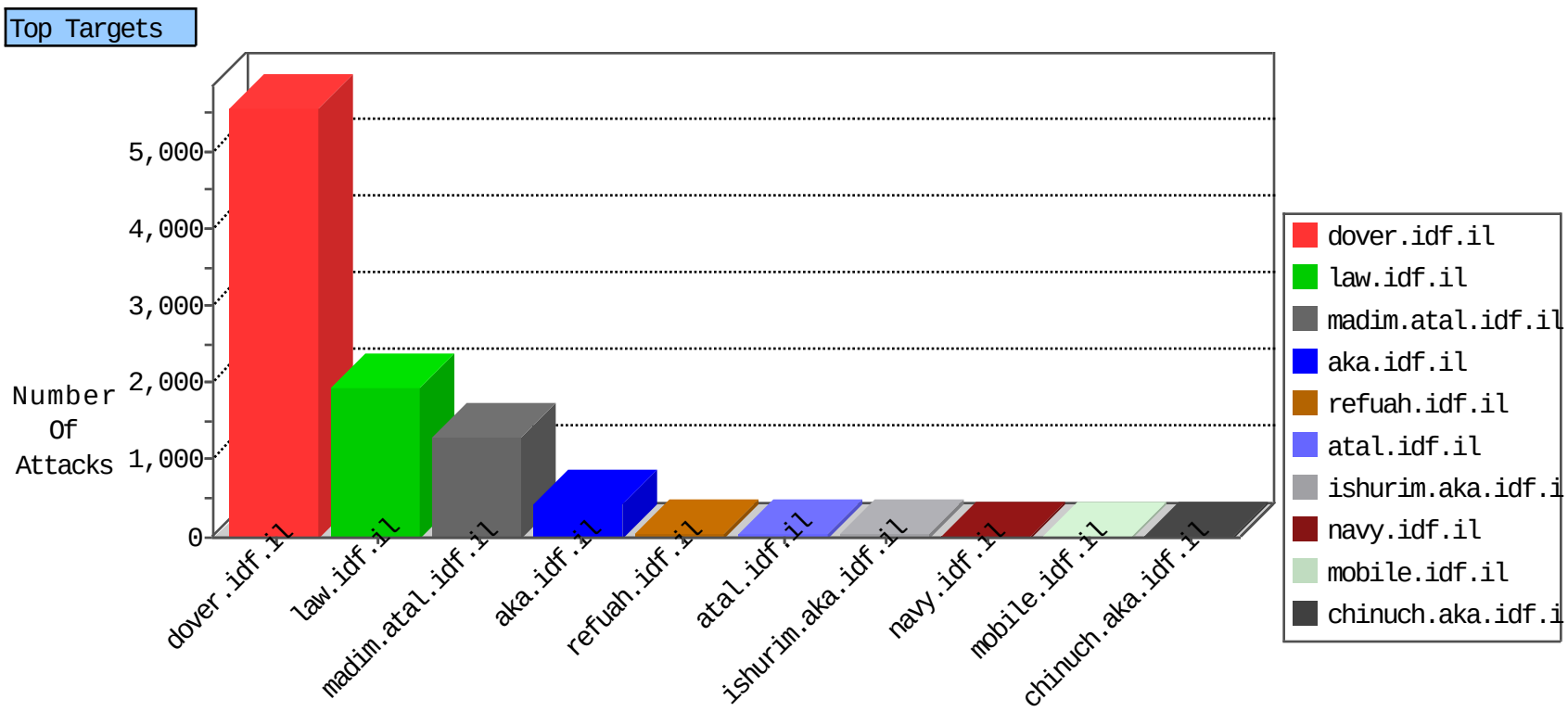
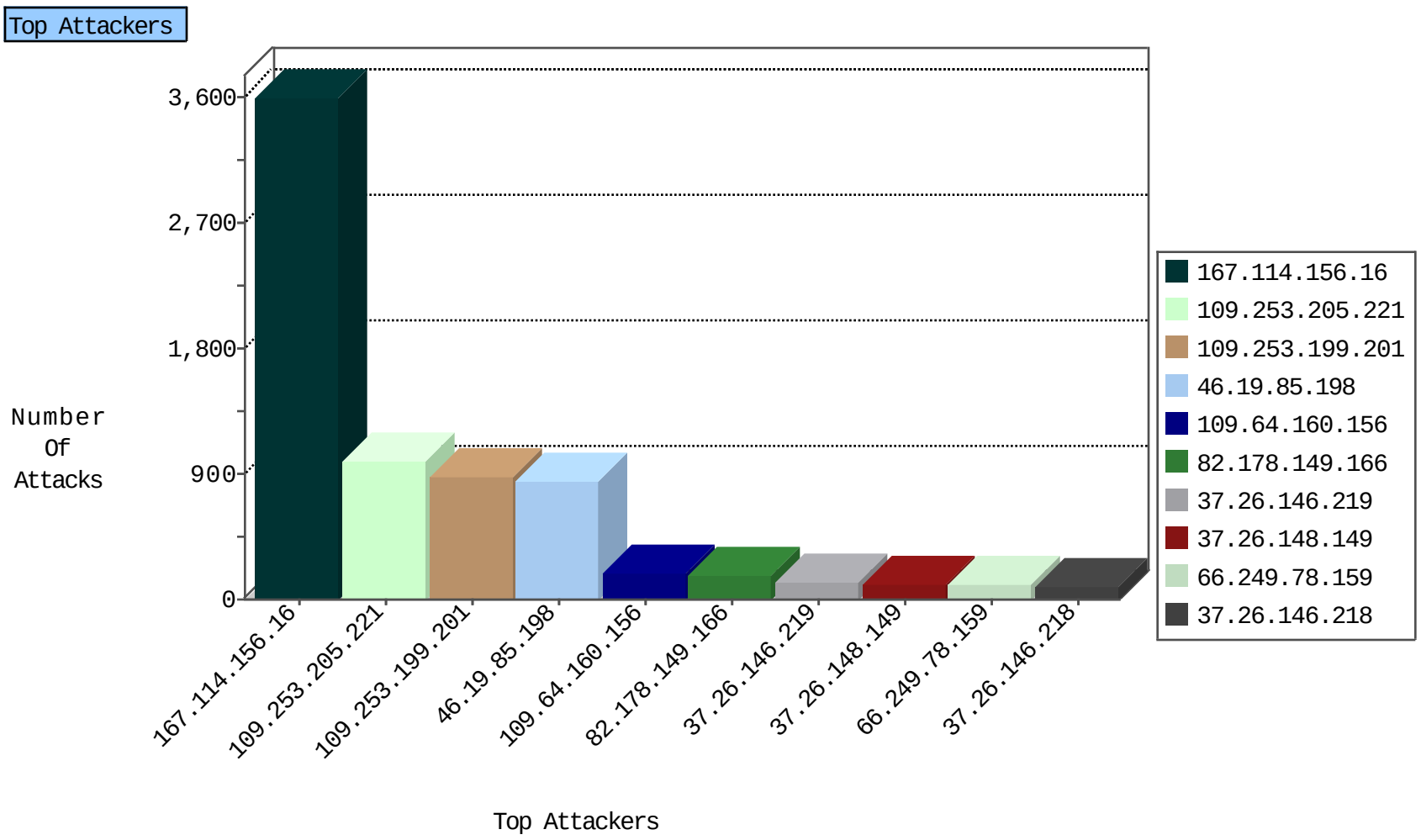
12-28-2015-10:04:06 to 12-28-2015-11:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-28-2015-10:04:06 to 12-28-2015-11:04:06

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	3405
37.26.148.149	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	91
37.26.146.219	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	89
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	85
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	77
37.26.146.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	66
66.249.81.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	61
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	59
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	50
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	44
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	38
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
66.249.66.25	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
37.26.146.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
85.181.180.186	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
88.182.114.67	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
185.89.216.230		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
82.213.2.174	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
65.19.138.34	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
155.91.64.11	Europe	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
37.26.146.144	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
199.30.16.184	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
162.243.57.54	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
37.26.148.236	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
37.26.146.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
66.249.66.31	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
203.133.169.77	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
63.141.204.25	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
37.26.148.241	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
105.196.147.226	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
37.26.148.236	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
185.89.216.237		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.26.146.141	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
104.131.240.186	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
185.89.216.230		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.26.148.149	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	7
89.169.98.152	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
37.26.148.180	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
37.26.146.141	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
140.234.253.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
105.196.147.226	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
65.19.138.34	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6

12-28-2015-10:04:06 to 12-28-2015-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-10:04:06 to 12-28-2015-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.178.149.166	147.237.77.216	Oman	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	44
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
216.177.129.99	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.77.178		e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.72.217		e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.183.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.201	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.175.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.77.170		maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.36	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.245.183.201	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
84.108.46.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.163.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-28-2015-10:04:06 to 12-28-2015-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1307
109.253.205.221	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	551
109.253.199.201	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	489
109.253.205.221	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	432
109.253.199.201	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	379
213.57.130.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	66
176.12.150.138	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
176.12.150.138	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
79.181.33.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	18
37.26.147.138	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.8.159.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
78.181.4.114	Turkey	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.146.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.178.178.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.18.53	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
46.19.85.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
105.196.147.226	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
178.152.190.227	Qatar	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
155.91.64.11	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.148.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
176.13.17.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.30.16.184	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.168.89.106	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
155.91.64.11	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.3.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
128.127.107.123	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.19.59	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.198.47	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.22.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

12-28-2015-10:04:06 to 12-28-2015-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	559
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.198	Block	164
109.64.160.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
82.178.149.166	Oman	147.237.77.216	dover.idf.il	Multiple Illegal Host Name from 82.178.149.166	Block	83
109.64.160.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.215.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
2.54.26.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.52.4.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
37.26.148.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
176.13.3.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
5.29.191.65	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
176.13.13.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
195.160.240.11	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	6
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	6
157.55.39.250	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	4
157.55.39.250	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on www.atal.idf.il/1133-he/imageserver.php	Block	4
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/6/	Block	3
176.13.17.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.127.107.123	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.147.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.172.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.90.25.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
46.19.85.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.12.140.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.0.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.237	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
194.90.25.122	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
31.168.84.143	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.192.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
213.57.228.231	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
78.181.4.114	Turkey	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
173.254.101.198	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.26.147.243	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
203.133.169.150	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
67.222.144.48	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.39	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on www.atal.idf.il/1133-he/imageserver.php	Block	1
109.253.137.83	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
80.246.136.218	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
185.27.105.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.5.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.158.150	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-28-2015-10:04:06 to 12-28-2015-11:04:06