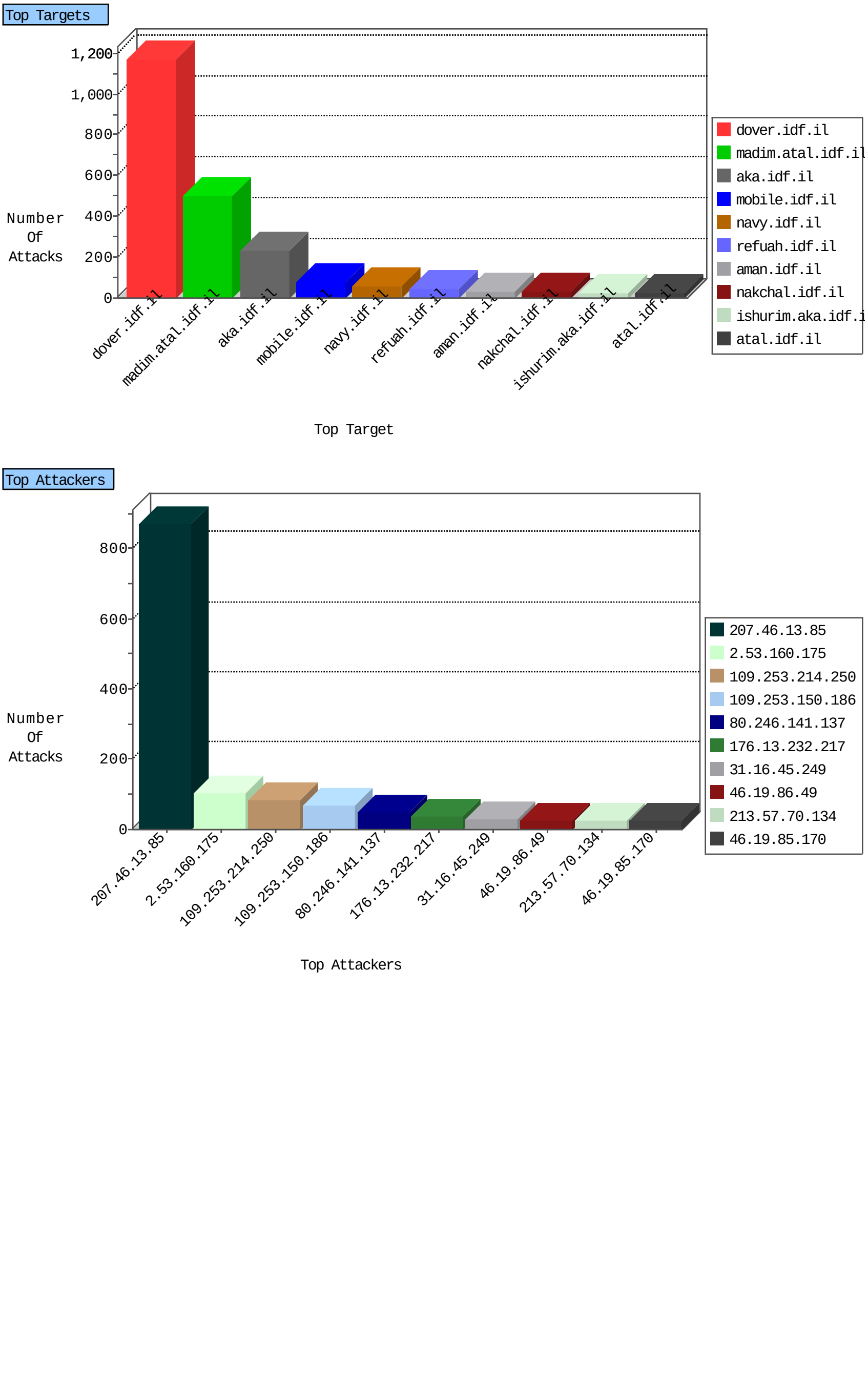
10-05-2016-10:04:01 to 10-05-2016-11:04:01

IDF Under Attack Daily Report



10-05-2016-10:04:01 to 10-05-2016-11:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.131	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
62.0.102.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
193.169.70.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
80.246.139.252	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.177.9.24	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
198.167.140.117	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
71.6.158.166	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
10.33.254.190		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
73.44.101.109	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-05-2016-10:04:01 to 10-05-2016-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.16.45.249	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	14
31.16.45.249	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
31.16.45.249	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
88.198.16.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
206.59.68.19	United States	147.237.77.121	e.navy.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1

10-05-2016-10:04:01 to 10-05-2016-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.90.189.128	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.33	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
194.90.88.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.91.21	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
180.150.177.188	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.31.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.149.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.195.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.185.218	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
54.90.212.162	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.154.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
194.152.9.215	147.237.77.216	Slovenia	dover.idf.il	portscan: TCP Distributed Portscan	1
46.229.223.8	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.120.124.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.91.20	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.167.169.71	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.121.219.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.98.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.148.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.77.214	147.237.72.167	Israel	ishurim.aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.188.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.150.189.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-05-2016-10:04:01 to 10-05-2016-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	866
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
213.57.70.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
62.0.212.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
62.0.220.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.180.44.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.87.104	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	11
100.92.227.212		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
2.53.39.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
95.35.78.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.215	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	9
2.55.0.191	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.173	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.53.49.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.254	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.252.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.213	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.164	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.166.190.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.254	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.18.184	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.160.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.246.137.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
91.135.102.162	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
86.104.160.82	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.236.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.66	Europe	147.237.76.42	refuah.idf.il	Directory Traversal	directory traversal overflow	monitor	4
46.19.86.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
5.102.242.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.160.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
109.253.214.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
109.253.150.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
80.246.141.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
176.13.232.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
80.246.139.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
185.32.179.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
185.32.179.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	9
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
212.179.162.246	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	9
80.246.140.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
80.246.139.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
80.246.139.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	7
185.32.179.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.242.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.139.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
77.125.51.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.140.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.238.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.179.162.246	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.179.162.246	Block	5
80.246.140.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
80.246.140.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.53.174.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.90.26.41	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
185.32.179.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.138.243.204	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.243.204	Block	3
80.246.140.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.140.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.70.243	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	3
80.246.140.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.221.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.35.78.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	2
80.246.139.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.139.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.160.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.139.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.2.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
2.53.160.175	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
145.253.174.210	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
77.138.243.204	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2

10-05-2016-10:04:01 to 10-05-2016-11:04:01