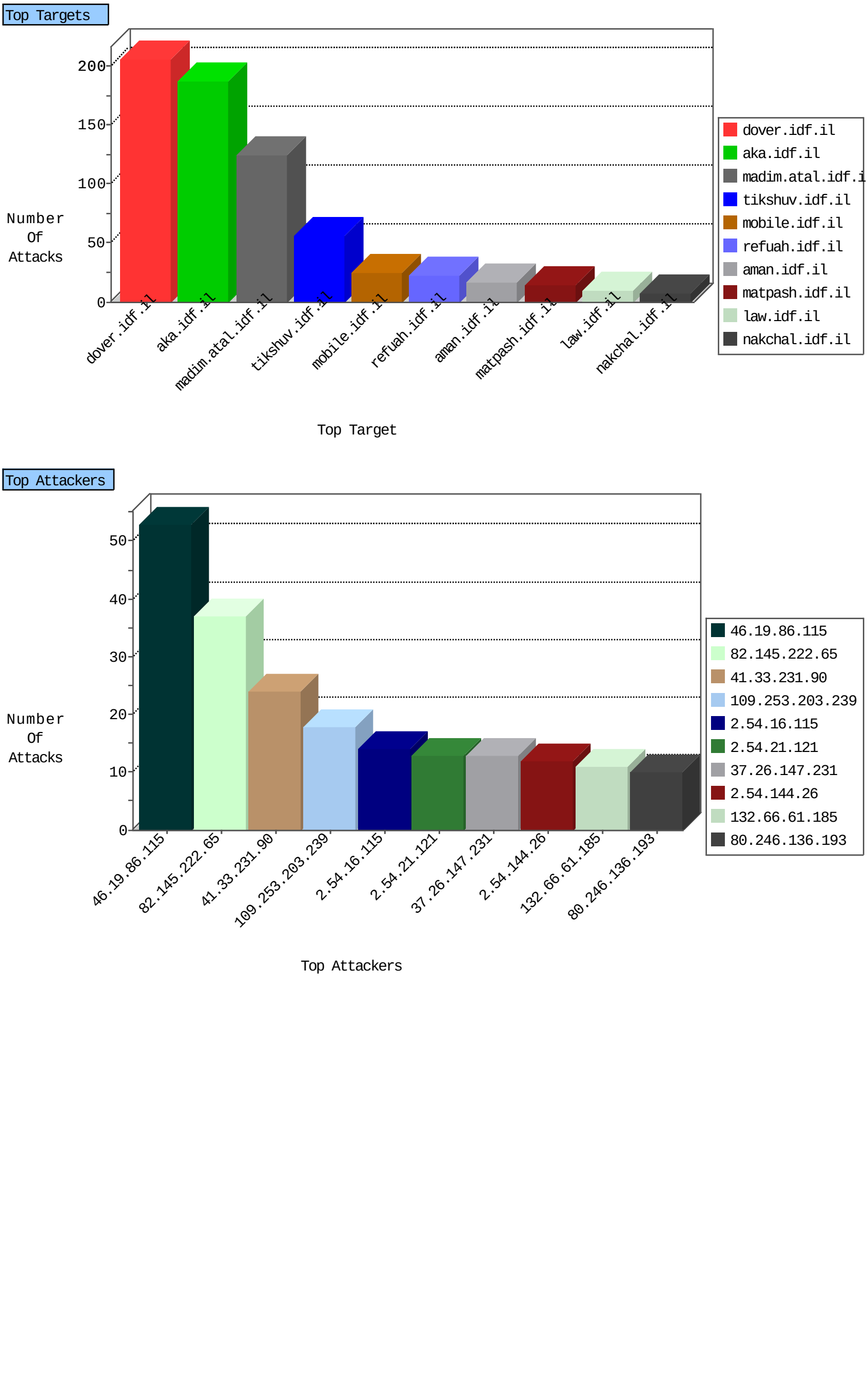
02-25-2016-13:04:06 to 02-25-2016-14:04:06

IDF Under Attack
Daily Report



02-25-2016-13:04:06 to 02-25-2016-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.222.65	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	37
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	2
198.23.190.39	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
198.23.190.39	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
198.23.190.39	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
181.211.161.231	Ecuador	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
181.211.161.231	Ecuador	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-25-2016-13:04:06 to 02-25-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.66.61.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
149.78.36.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
95.86.112.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
188.120.148.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.176.7.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
217.132.137.39	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.146.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
194.90.169.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.235.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.147	Italy	147.237.76.147	chinuch.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
94.230.93.211	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
162.219.4.147	United States	147.237.76.31	nakchal.idf.il	C1000016: HTTP: administrator in URI	Block	1

02-25-2016-13:04:06 to 02-25-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.203.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
82.80.17.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.207.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.172.21.120	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
212.34.12.119	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.12.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.217.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.76.176	Romania	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.23.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.230.16.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.176.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.10.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.145.251.121	147.237.77.61	China	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.253.195.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.62.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-25-2016-13:04:06 to 02-25-2016-14:04:06

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	24
82.213.48.51	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
80.246.136.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.54.187.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
82.80.154.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.144.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.16.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.130.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.54.21.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.120.73.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.191.117	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
82.166.93.161	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
46.19.85.155	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.15.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.57.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.132.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.80.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.148.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.201.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.24.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.171.128.165	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.138.160	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
85.65.24.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.168.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.68.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.176.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.94.100.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.29.211.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.135.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.109.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.53.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.138.160	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
194.90.209.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.101.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.199.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-25-2016-13:04:06 to 02-25-2016-14:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.178.102.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-25-2016-13:04:06 to 02-25-2016-14:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.203.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.54.21.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.89.217.224		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.89.217.228		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
46.19.85.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.121.60.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.89.217.227		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.89.217.232		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	2
162.219.4.147	United States	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	2
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.191	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
185.89.217.230		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
84.109.17.62	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
2.54.51.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.89.217.231		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
162.219.4.147	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 162.219.4.147	Block	1
2.54.136.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.136.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
180.76.15.135	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9364-he/refuah.aspx	Block	1
37.26.146.151	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
207.46.13.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspx„'ƒ„,„¯ƒλ€Š„,„¿„ƒ„'•'½„,„Š€λƒ„'„,„¯ƒλ€Š„,„¿„ƒ„'½„,„Š€λƒ„'„,„¯ƒλ€Š„,„	Block	1
93.113.125.11	Romania	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1
46.210.212.195	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.237.172.59	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.204.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.39.222.159	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/rom-0	Block	1
213.57.158.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
185.89.217.233		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
185.13.47.166	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/rabanut/general.aspx	None	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.52.164.245	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.25.112.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.49.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.89.217.229		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
162.219.4.147	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/wp-login.php	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	1
109.253.219.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.13.112.116	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.234		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1

02-25-2016-13:04:06 to 02-25-2016-14:04:06