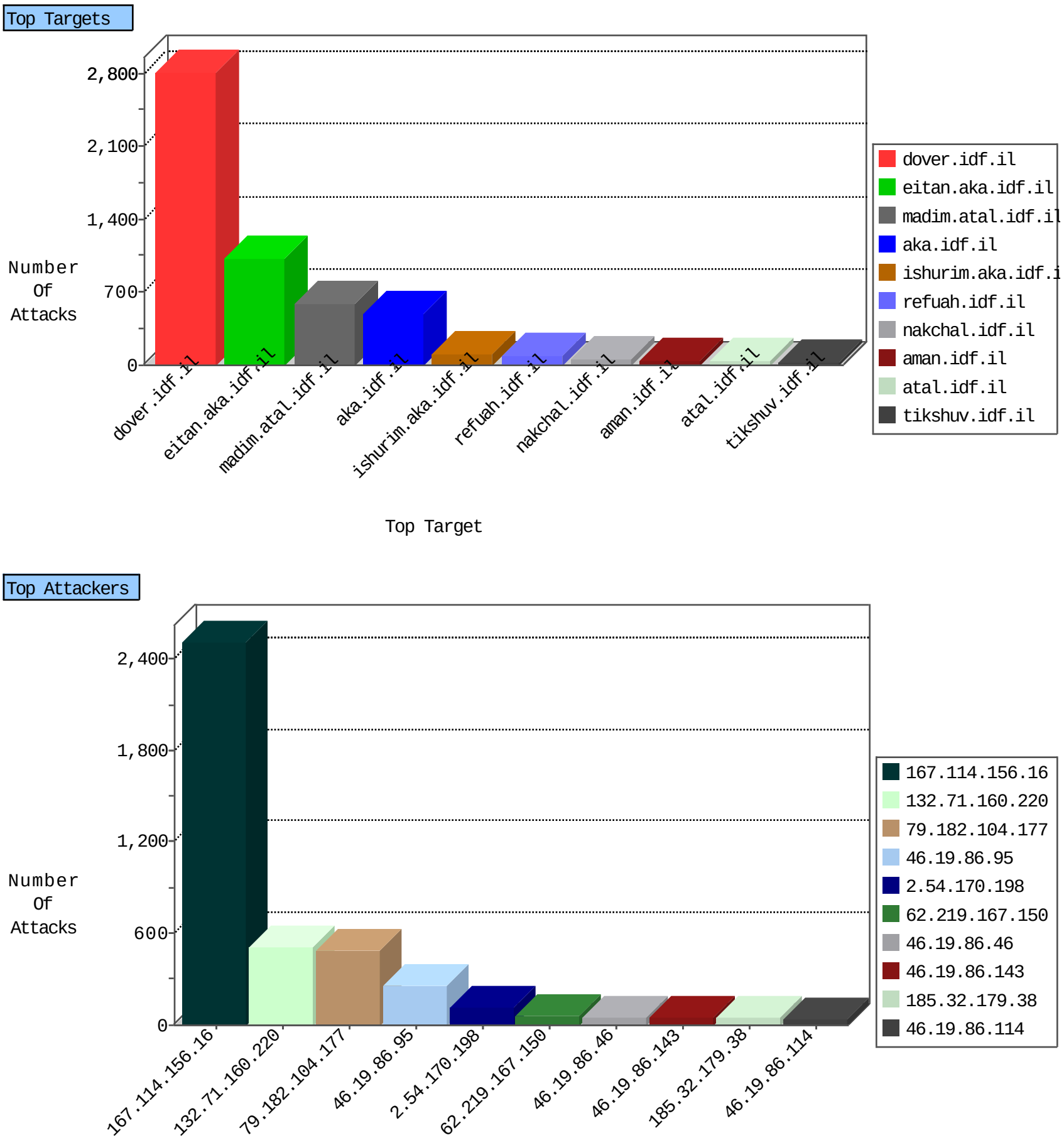
12-02-2015-10:04:07 to 12-02-2015-11:04:07

IDF Under Attack
Daily Report



12-02-2015-10:04:07 to 12-02-2015-11:04:07

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	3374
93.174.93.151	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
188.114.21.201	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-02-2015-10:04:07 to 12-02-2015-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.211.20	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-02-2015-10:04:07 to 12-02-2015-11:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.159.253	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.136.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.211.20	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.40.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.224.8	147.237.76.200	Ukraine	eitan.aka.idf.il	SERVER-WEBAPP admin.php access	1
185.106.94.46	147.237.0.15		kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
159.147.148.28	147.237.76.177	Spain	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.20.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.183.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.16.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.21.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.186.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.46	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.155	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1

12-02-2015-10:04:07 to 12-02-2015-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.104.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	441
132.71.160.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.86.46	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
213.55.104.103	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
62.219.167.150	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
62.219.167.150	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
100.100.123.64		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.166.188.209	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
80.246.130.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.86.96	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
93.173.32.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
100.100.85.133		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.47.29		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.50	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
100.100.123.64		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
94.230.86.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.52.28.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.173.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.183.55.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
100.100.41.192		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
80.246.133.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.143.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.32.179.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.153.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.136.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.115.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.93.210	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
2.52.182.101	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.93.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.235.80.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.0.240.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.185.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

12-02-2015-10:04:07 to 12-02-2015-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.71.160.220	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	464
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.95	Block	113
2.54.170.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
185.32.179.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
79.182.104.177	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
176.13.10.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
80.246.136.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
87.69.181.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
185.32.179.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
77.127.151.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
62.90.92.170	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.90.92.170	Block	9
197.37.10.159	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	8
197.37.10.159	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	8
213.151.36.130	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/&sa=u&ved=0ahukewj59-a_6lzjahudwrokha6qb_uqfggrmam&usg=afqjcnhsjqzgxohl-8ga1aemjbw8wkvaxw	Block	7
80.246.136.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.27.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.28.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.170.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
193.201.224.8	Ukraine	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	2
176.12.143.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.2.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.166.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
193.201.224.8	Ukraine	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 193.201.224.8	Block	2
79.181.17.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.93.191	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
46.19.85.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.121.154.90	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
80.246.133.78	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.121.154.90	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
95.86.108.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/&sa=u&ved=0ahukewibx8xr3lzjahxbpxqkhezoaxuqfggkmae&usg=afqjcnfd5s02zieedmbmfxvss2_oefusww	Block	1
5.29.143.128	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
207.46.13.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
2.54.161.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/15092010masaiyot.aspx	Block	1
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.219.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
80.250.154.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.90.92.170	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.159.253	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	1
46.121.154.90	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 1	Block	1
132.71.160.220	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1

12-02-2015-10:04:07 to 12-02-2015-11:04:07