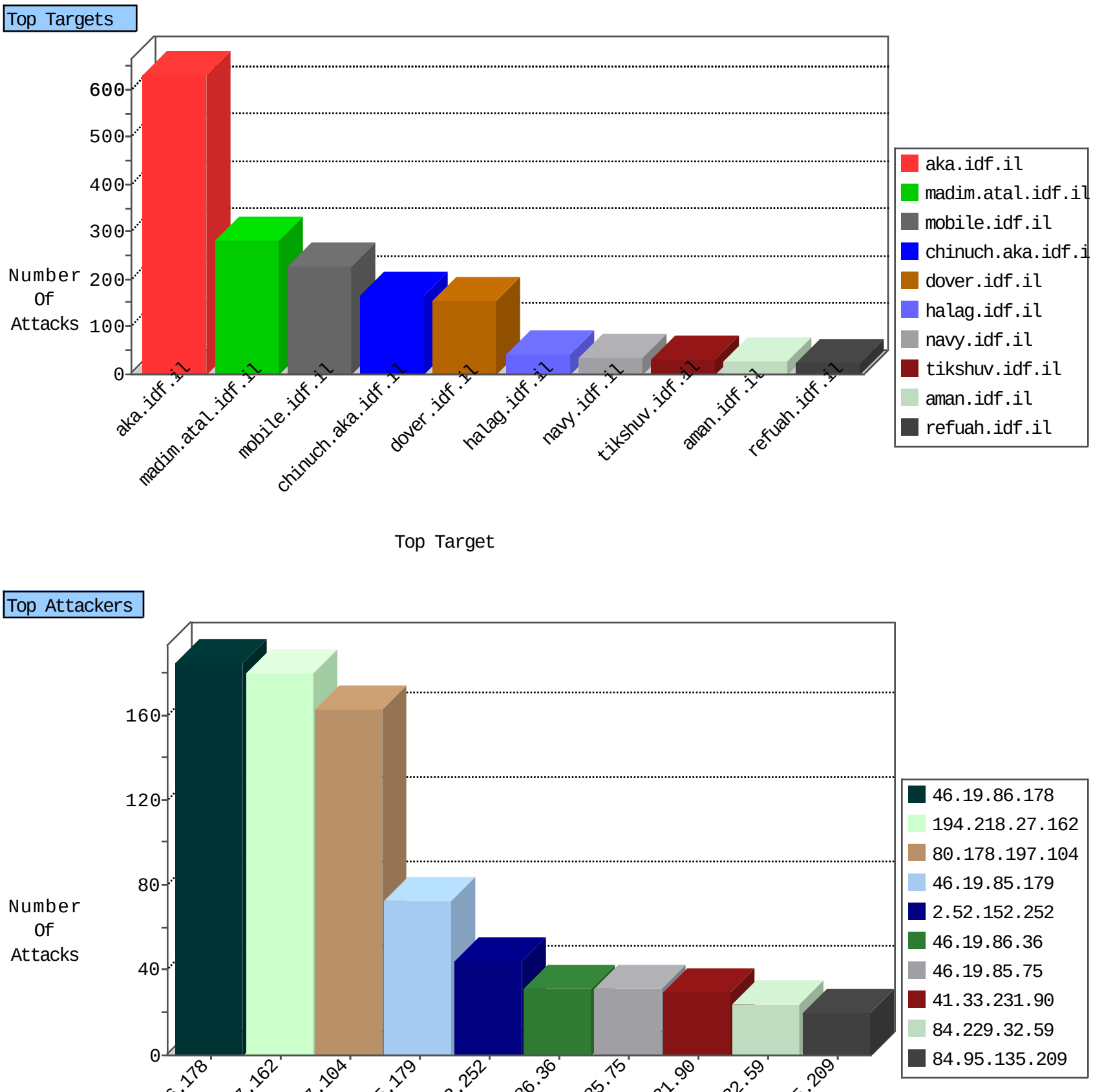
02-29-2016-22:04:06 to 02-29-2016-23:04:06

IDF Under Attack
Daily Report



02-29-2016-22:04:06 to 02-29-2016-23:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.233.69	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.130.5.201		147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.162	China	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

02-29-2016-22:04:06 to 02-29-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
109.66.196.153	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.116.2.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
217.132.153.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.90.118	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2

02-29-2016-22:04:06 to 02-29-2016-23:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.90	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
109.65.54.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.130.13.220	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
84.108.123.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
71.203.129.11	147.237.76.42	United States	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
183.61.109.189	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
36.37.226.117	147.237.76.148	Cambodia	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
183.61.109.189	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
112.74.39.155	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.170.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.13.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.119.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.108.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.215	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
36.37.226.117	147.237.76.148	Cambodia	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
183.61.109.189	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
5.28.184.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.227.64.115	147.237.77.205	Taiwan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
112.74.39.155	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

02-29-2016-22:04:06 to 02-29-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.178.197.104	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
46.19.85.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.52.152.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.229.32.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
84.95.135.209	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
37.26.146.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.62.201.143	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.22.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.69.8	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.65.80.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.241.251.3	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.228.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.182.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.71.41.90	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
109.253.200.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.136.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.134.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.80.132.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.70.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.92.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.27.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.55.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.243.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.210.250	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.59.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.12.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.252.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.115.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.164.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.168.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.241.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.35.61	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.92.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.195.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.174.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

02-29-2016-22:04:06 to 02-29-2016-23:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.22.135.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.130.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.181.130.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

02-29-2016-22:04:06 to 02-29-2016-23:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	185
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
37.26.146.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
2.52.152.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
37.26.146.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.68	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	4
176.13.22.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.71	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	3
84.108.182.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
46.121.214.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.32.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.125.242.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.4.169	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	3
109.253.145.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.75	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	3
176.241.251.3	France	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.183.174.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
162.245.144.163	Canada	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
37.26.146.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.80.48	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.65.80.48	Block	2
109.253.136.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.72	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
46.117.247.101	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
109.66.6.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
66.249.66.78	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
109.64.105.140	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
84.95.135.209	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.120.43.43	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	NULL Character in Header Name at À*À&À[[#15]]À[[#5]][[#0]]k[[#0]]j[[#0]]9[[#0]]8À'À#À[[#19]]À#011À)À%À[[#14]]À[[#4]][[#0]]g[[#0]]@[[#0]]3[[#0]]2À[[#18]]À[[#8]]À#012À[[#3]][[#0]]ˆ[[#0]]‡[[#0]]E[[#0]]D[[#0]][[#22]][[#0]][[#19]][[#0]]•[[#0]]œ[[#0]]=[[#0]]5[[#0]]<[[#0]]/[[#0]]„[[#0]]A[[#0]]	Block	1
156.199.197.226		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.179.4.169	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod http:/news.nana10.co.il/article/	Block	1
40.77.167.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/main/home/default.aspx	Block	1
109.67.3.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.3.55	Block	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
192.241.179.165	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
5.28.135.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
94.23.57.83	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name [[#0]]ÿ[[#1]][[#0]][[#1]]c[[#0]][[#0]][[#0]][[#20]][[#0]][[#18]][[#0]][[#0]][[#15]]www.aman.idf.il[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1
138.36.0.3		147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/index.php	Block	1
66.249.66.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx	Block	1
2.54.55.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.121.65.203	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.32.179.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]#õ"!û8[[#3]]PàÖÄc£•.[[#7]]<_XC{"Œ–êál'×[[#5]]ï [[#0]][[#0]]pÀ0À,À2À.À/À+À1À-[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]žÀ(À$À[[#20]]À	Block	1
157.55.39.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

02-29-2016-22:04:06 to 02-29-2016-23:04:06