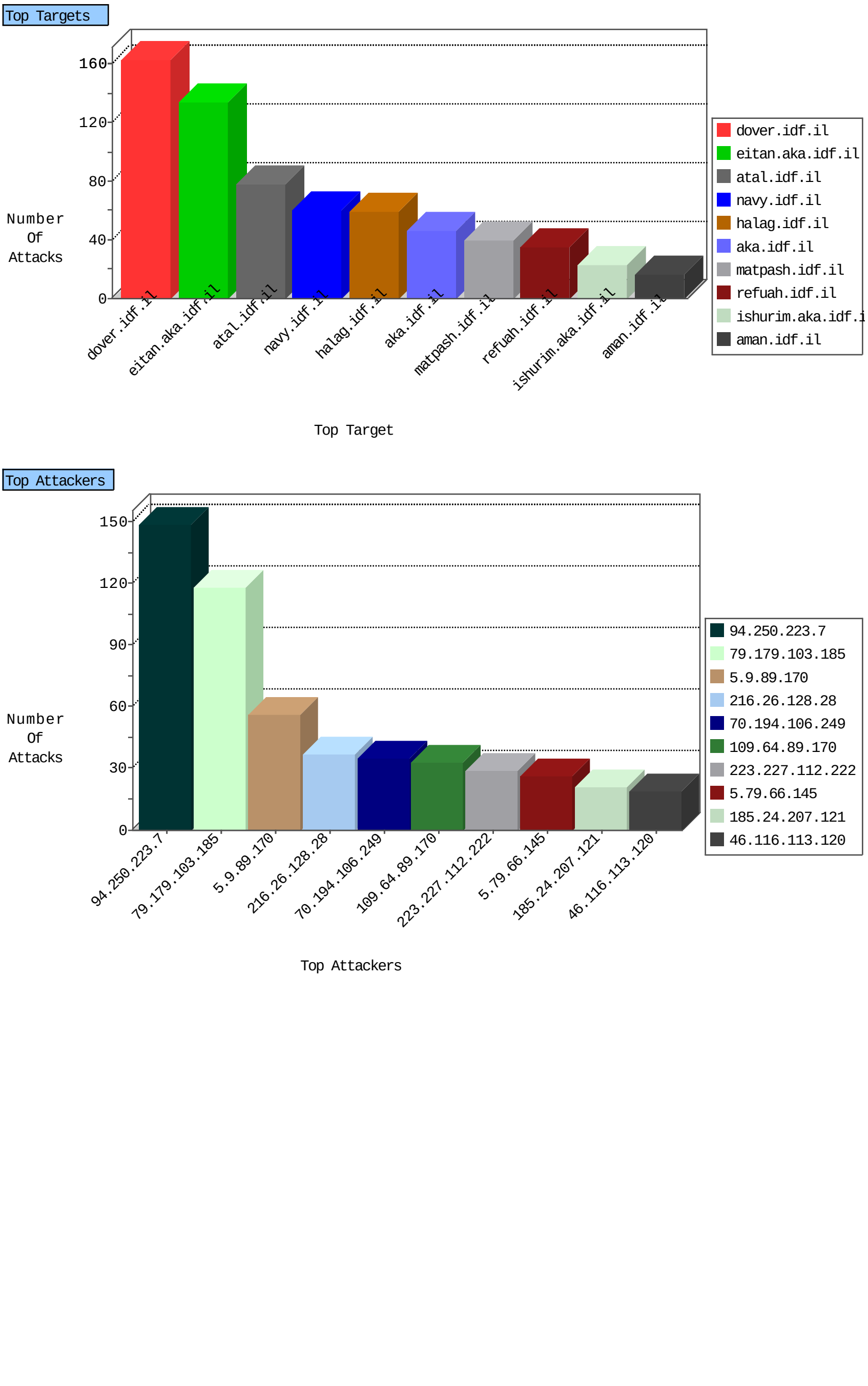
09-09-2016-23:04:04 to 09-10-2016-00:04:04

IDF Under Attack
Daily Report



09-09-2016-23:04:04 to 09-10-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.139.135.129	United States	147.237.77.226	www.chamatz.aka.idf.il	Invalid TCP Flags	drop	1
98.139.135.129	United States	147.237.77.235	sviva.idf.il	Invalid TCP Flags	drop	1
98.139.135.129	United States	147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
98.139.135.129	United States	147.237.77.205	prisha.idf.il	Invalid TCP Flags	drop	1
187.108.192.90	Brazil	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

09-09-2016-23:04:04 to 09-10-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	49
216.26.128.28	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
216.26.128.28	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.26.128.28	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
195.8.208.130	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
23.96.97.203	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
23.96.97.235	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
5.9.89.170	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
23.96.97.233	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
195.8.208.130	Netherlands	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-09-2016-23:04:04 to 09-10-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.26.128.28	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
195.8.208.130	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	8
23.96.97.203	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
108.166.190.139	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
23.96.97.235	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
23.96.97.233	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	2
93.158.203.147	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.76.196	Sweden	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.92.20.154	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.168.200	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.149	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.76.201	Sweden	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
163.172.129.15	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.160.132	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.64.56.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.186.20.183	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

09-09-2016-23:04:04 to 09-10-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.103.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	80
109.64.89.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
70.194.106.249	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.79.66.145	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
79.179.103.185	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
79.179.103.185	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
213.174.55.11	Germany	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	18
46.116.113.120	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
213.57.54.206	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
223.227.112.222	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.24.207.121	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
100.92.100.105		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
74.91.125.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
94.250.223.7	Germany	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
94.250.223.7	Germany	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
94.250.223.7	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
94.250.223.7	Germany	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
94.250.223.7	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.239.234	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
94.250.223.7	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
94.250.223.7	Germany	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
94.250.223.7	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
94.250.223.7	Germany	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
94.250.223.7	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
94.250.223.7	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
94.250.223.7	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
94.250.223.7	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
223.227.112.222	India	147.237.77.216	dover.idf.il	SYN Attack		monitor	6
223.227.112.222	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
70.194.106.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.250.223.7	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
70.194.106.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.250.223.7	Germany	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.24.207.121	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.120.63.177	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.116.91.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.239.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
138.246.253.19	Germany	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.79.66.145	Netherlands	147.237.76.86	navy.idf.il	SYN Attack		monitor	4
109.65.66.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.27.106.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.150.128.142	Italy	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-09-2016-23:04:04 to 09-10-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.166.81	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 79.180.166.81	Block	4
46.19.85.3	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method d4q3o in URL	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
77.124.41.213	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.108.7.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
46.116.113.120	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
144.76.16.162	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
77.139.49.133	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/tizmoret/gallery/	Block	1
2.53.182.108	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.71.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.71.34.241	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
180.76.15.26	China	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
79.176.1.161	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.142.231.97	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
89.138.222.85	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
185.27.106.126	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/categorytemplates/listchildcategories/2080	Block	1
79.180.166.81	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Value at 1 for www.aman.idf.il/modiin/questionnaires.aspx	Block	1
46.19.85.3	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
109.64.89.170	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1

09-09-2016-23:04:04 to 09-10-2016-00:04:04